DEPARTMENT OF DEFENSE

DEFENSE SCIENCE BOARD

TASK FORCE REPORT:

Resilient Military Systems and the Advanced Cyber Threat

January 2013

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY AND LOGISTICS
WASHINGTON, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

The DSB Task Force on Resilient Military Systems and the Advanced Cyber Threat completed its information gathering in August 2012.

This report is UNCLASSIFIED and releasable to the public.

DEFENSE SCIENCE BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

October 11, 2012

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY & LOGISTICS

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Resilient Military Systems

I am pleased to forward the final report of the DSB Task Force on Resilient Military Systems. This study comprises one part of a DSB Cyber Initiative. A study on Cyber-Security and Reliability in a Digital Cloud is the other component of the initiative and will be forwarded shortly.

The Task Force on Resilient Military Systems provides a set of recommendations to improve the resilience of DoD systems to cyber attacks. The overarching strategy aims to enhance the Department's defenses against known vulnerabilities; decrease the effectiveness of, and increase the cost to, adversaries attempting to introduce new vulnerabilities; and deter the most sophisticated actors by ensuring the US maintains the ability to deliver desired mission capabilities in the face of a catastrophic cyber attack.

In addition, the Task Force identified a framework to implement a metrics collection system and then develop appropriate performance metrics that can be used to shape the Department's investment decisions. The framework can be adjusted to accommodate alternative implementation plans and should prove a powerful tool for the Department's leadership.

I fully endorse all of the Task Force's recommendations contained in this report, and urge their careful consideration and soonest adoption.

Paul A. Kaminski

Dr. Paul Kaminski
Chairman

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

DEFENSE SCIENCE
BOARD

October 10, 2012

MEMORANDUM TO THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Resilient Military Systems

The final report of the DSB Task Force on Resilient Military Systems is attached. This report is based on the perspective of 24 Task Force members who received more than 50 briefings from practitioners and senior officials throughout the Department of Defense (DoD), Intelligence Community (IC), commercial sector, academia, national laboratories, and policymakers.

This Task Force was asked to review and make recommendations to improve the resilience of DoD systems to cyber attacks, and to develop a set of metrics that the Department could use to track progress and shape investment priorities.

After conducting an 18-month study, this Task Force concluded that the cyber threat is serious and that the United States cannot be confident that our critical Information Technology (IT) systems will work under attack from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with all of their military and intelligence capabilities (a "full spectrum" adversary). While this is also true for others (e.g. Allies, rivals, and public/private networks), this Task Force strongly believes the DoD needs to take the lead and build an effective response to measurably increase confidence in the IT systems we depend on (public and private) and at the same time decrease a would-be attacker's confidence in the effectiveness of their capabilities to compromise DoD systems. This conclusion was developed upon several factors, including the success adversaries have had penetrating our networks; the relative ease that our Red Teams have in disrupting, or completely beating, our forces in exercises using exploits available on the Internet; and the weak cyber hygiene position of DoD networks and systems. The Task Force believes that the recommendations of this report create the basis for a strategy to address this broad and pervasive threat.

Nearly every conceivable component within DoD is networked. These networked systems and components are inextricably linked to the Department's ability to project military force and the associated mission assurance. Yet, DoD's networks are built on inherently insecure architectures that are composed of, and increasingly using, foreign parts. While DoD takes great care to secure the use and operation of the "hardware" of its weapon systems, the same level of resource and attention is not spent on the complex network of information technology (IT) systems that are used to support and operate those weapons or critical IT capabilities embedded within them.

DoD's dependence on this vulnerable technology is a magnet to U.S. opponents. In fact, DoD and its contractor base have already sustained staggering losses of system design information incorporating decades of combat knowledge and experience that provide adversaries insight to

technical designs and system use. Despite numerous DoD actions, efforts are fragmented, and the Department is not currently prepared to effectively mitigate this threat.

Cyber is a complicated domain. There is no silver bullet that will eliminate the threats inherent to leveraging cyber as a force multiplier, and it is impossible to completely defend against the most sophisticated cyber attacks. However, solving this problem is analogous to complex national security and military strategy challenges of the past, such as the counter U-boat strategy in WWII and nuclear deterrence in the Cold War. The risks involved with these challenges were never driven to zero, but through broad systems engineering of a spectrum of techniques, the challenges were successfully contained and managed. Similarly, by employing the systems approach detailed in the report, the Task Force believes the Department can effectively manage and contain the risks presented by the cyber threat.

The report details an overall risk reduction strategy, which includes a combination of deterrence, refocused intelligence capabilities, and an improved cyber defense. Pursuing this strategy will enable the Department to credibly defend against known vulnerabilities; decrease the effectiveness of, and increase the cost to, adversaries attempting to introduce new vulnerabilities; and deter the most sophisticated actors by ensuring the US has a critical set of segmented conventional systems that will deliver desired mission capabilities in the face of a catastrophic attack. Taking these steps will provide DoD with a ladder of capabilities, ensuring the President has multiple response options to a catastrophic cyber attack. It also removes the requirement to protect all of our military systems from the most advanced cyber threats, which the Task Force believes is neither feasible nor affordable.

In addition, while the Task Force did not find metrics available today to directly determine or predict the cyber security or resilience of a given system, the Task Force was able to create an implementation plan to develop measurement systems to help the Department execute the proposed risk reduction strategy and then measure performance within that structure.

Ultimately, this Task Force report makes a case for implementing a broad systems approach (that is grounded in its technical and economic feasibility) to effectively address the cyber threat. It will take time to build the capabilities necessary to prepare and protect our country from present and future cyber threats, therefore DoD must act now.

We fully endorse all of the recommendations made in this report and urge their adoption.

Mr. James R. Gosler
Co-Chair

Mr. Lewis Von Thaer
Co-Chair

Table of Contents

List of Figures

List of Tables

Executive Summary

The United States cannot be confident that our critical Information Technology (IT) systems will work under attack from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with all of their military and intelligence capabilities (a "full spectrum" adversary). While this is also true for others (e.g. Allies, rivals, and public/private networks), this Task Force strongly believes the DoD needs to take the lead and build an effective response to measurably increase confidence in the IT systems we depend on (public and private) and at the same time decrease a would-be attacker's confidence in the effectiveness of their capabilities to compromise DoD systems. We have recommended an approach to do so, and we need to start now!

While DoD takes great care to secure the use and operation of the “hardware” of its weapon systems, these security practices have not kept up with the cyber adversary tactics and capabilities. Further, the same level of resource and attention is not spent on the complex network of information technology (IT) systems that are used to support and operate those weapons or critical cyber capabilities embedded within them. This Task Force was asked to review and make recommendations to improve the resilience of DoD systems to cyber attacks and to develop a set of metrics that the Department could use to track progress and shape investment priorities.

Over the past 18 months, the Task Force received more than 50 briefings from practitioners and senior officials throughout the DoD, Intelligence Community (IC), commercial practitioners, academia, national laboratories, and policymakers. As a result of its deliberations, the Task Force concludes that:

- The cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War
- The cyber threat is also insidious, enabling adversaries to access vast new channels of intelligence about critical U.S. enablers (operational and technical; military and industrial) that can threaten our national and economic security
- Current DoD actions, though numerous, are fragmented. Thus, DoD is not prepared to defend against this threat
- DoD red teams, using cyber attack tools which can be downloaded from the Internet, are very successful at defeating our systems
- U.S. networks are built on inherently insecure architectures with increasing use of foreign-built components
- U.S. intelligence against peer threats targeting DoD systems is inadequate
- With present capabilities and technology it is not possible to defend with confidence against the most sophisticated cyber attacks
- It will take years for the Department to build an effective response to the cyber threat to include elements of deterrence, mission assurance and offensive cyber capabilities.

Report Terminology

To discuss the cyber threat and potential responses in more detail, it is important to establish some common language. For purpose of this report, **Cyber** is broadly used to address the components and systems that provide all digital information, including weapons/battle management systems, IT systems, hardware, processors, and software operating systems and applications, both standalone and embedded. **Resilience** is defined as the ability to provide acceptable operations despite disruption: natural or man-made, inadvertent or deliberate. **Existential Cyber Attack** is defined as an attack that is capable of causing sufficient wide scale damage for the government potentially to lose control of the country, including loss or damage to significant portions of military and critical infrastructure: power generation, communications, fuel and transportation, emergency services, financial services, etc.

The Task Force developed a threat hierarchy to describe capabilities of potential attackers, organized by level of skills and breadth of available resources (See Figure ES.1).

- Tiers I and II attackers primarily *exploit known* vulnerabilities
- Tiers III and IV attackers are better funded and have a level of expertise and sophistication sufficient to *discover new* vulnerabilities in systems and to exploit them
- Tiers V and VI attackers can invest large amounts of money (billions) and time (years) to *actually create* vulnerabilities in systems, including systems that are otherwise strongly protected.

Higher-tier competitors will use all capabilities available to them to attack a system but will usually try lower-tier exploits first before exposing their most advanced capabilities. Tier V and VI level capabilities are today limited to just a few countries such as the United States, China[1],[2] and Russia.[3]

[1] Office of the National Intelligence Executive; "Foreign Spies Stealing US Economic Secrets in Cyber Space: Report to Congress on Foreign Economic Collection and Industrial Espionage;" 2011

[2] Gen Keith Alexander; testimony to US Senate Armed Services Committee on US Strategic Command and US Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2013; Tuesday, March 27, 2012

[3] Maneki, Sharon; "Learning from the Enemy: The Gunman Project;" Center for Cryptologic History, National Security Agency; 2009

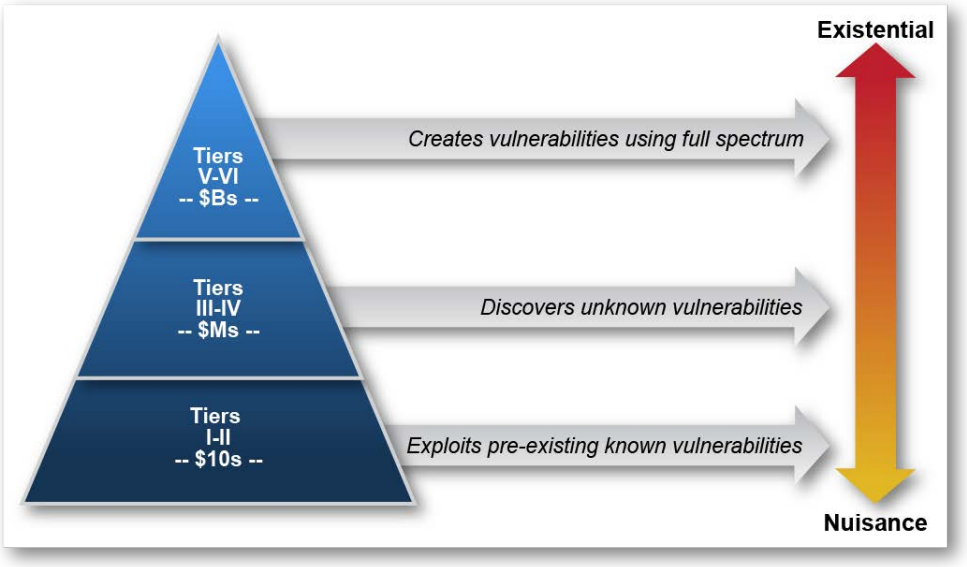

Figure ES.1 Cyber Threat Taxonomy

Background

The adversary is in our networks. Then Deputy Secretary of Defense William Lynn's 2010 Foreign Affairs article documented a significant compromise of DoD classified networks in 2008 through the simple insertion of an infected flash drive. Moreover, adversaries exploit more than military operational systems, but intellectual property relevant to our commercial industries as well.

The DoD, and its contractor base are high priority targets that have sustained staggering losses of system design information incorporating years of combat knowledge and experience. Employing reverse engineering techniques, adversaries can exploit weapon system technical plans for their benefit. Perhaps even more significant, they gained insight to operational concepts and system use (e.g., which processes are automated and which are person controlled) developed from decades of U.S. operational and developmental experience—the type of information that cannot simply be recreated in a laboratory or factory environment. Such information provides tremendous benefit to an adversary, shortening time for development of countermeasures by years.

In addition, there is evidence of attacks that exploit known vulnerabilities in the domestic power grid and critical infrastructure systems.[4,5] DoD, and the United States, is extremely reliant on the availability of its critical infrastructure.

[4] US-Canada Power System Outage Task Force Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations; April 2004; Excerpt from report: "The generation and delivery of electricity has been, and continues to be, a target of malicious groups and individuals intent on disrupting this system. Even attacks that do not directly target the electricity sector can have disruptive effects on electricity

Exploitation is not a new threat. For years adversaries have infiltrated U.S. systems, sometimes detected, sometimes deflected, but almost never deterred. A recently declassified Soviet Union operation against the United States serves as an effective example. Starting in the late 1970s, the Gunman operation exploited an operationally introduced vulnerability resulting in the transmission to Soviet intelligence of every keystroke in 16 IBM Selectric typewriters located in the U.S. Embassy in Moscow and the U.S. Mission in Leningrad. More recently, in 2010, the 2nd International Conference on Information Engineering and Computer Science (ICIECS), published an article titled "Towards Hardware Trojan: Problem Analysis and Trojan Simulation" authored by members of the Department of Computer Science and Technology Zhengzhou Institute of Information Science and Technology, in Zhengzhou, China which outlined the technical approach elements for developing covertly modified hardware. The concept of hardware modification is so prevalent now that criminal elements routinely insert modified or replacement card readers to steal customer information from automated teller machines (ATMs), and other commercial activities.

Recent DoD and U.S. interest in counterfeit parts has resulted in the identification of widespread introduction of counterfeit parts into DoD systems through commercial supply chains. Since many systems use the same processors and those processors are typically built overseas in untrustworthy environments, the challenge to supply chain management in a cyber-contested environment is significant.

Identification of operationally introduced vulnerabilities in complex systems is extremely difficult technically, and as a result, cost prohibitive. The United States only learned of Project GUNMAN via a tipoff from a liaison intelligence service. The ability of intelligence to provide unique and specific information provides some mitigation against a Tier V-VI adversary's ability to introduce vulnerabilities.

DoD is in the process of institutionalizing a Supply Chain Risk Management (SCRM) strategy that prioritizes scarce security resources on critical mission systems and components, provides intelligence analysis to acquisition programs and incorporates vulnerability risk mitigation requirements into system designs.

The success of DoD red teams against its operational systems should also give pause to DoD leadership. During exercises and testing, DoD red teams, using only small teams and a short amount of time, are able to significantly disrupt the "blue team's" ability to carry out military

system operations. Many malicious code attacks, by their very nature, are unbiased and tend to interfere with operations supported by vulnerable applications. One such incident occurred in January 2003, when the "Slammer" Internet worm took down monitoring computers at FirstEnergy Corporation's idled Davis-Besse nuclear plant. A subsequent report by the North American Electric Reliability Council (NERC) concluded that although the infection caused no outages, it blocked commands that operated other power utilities."

[5] In the Crossfire Critical Infrastructure in the Age of Cyber War; 2010 joint study between McAfee and CSIS

missions. Typically, the disruption is so great, that the exercise must be essentially reset without the cyber intrusion to allow enough operational capability to proceed. These stark demonstrations contribute to the Task Force's assertion that the functioning of DoD's systems is not assured in the presence of even a modestly aggressive cyber attack.

The DSB 2010 Summer Study addressed the issue of degraded operations and the need to include cyber attacks in realistic exercises. The Chairman, Joint Chiefs of Staff, issued an instruction in February 2011[6] mandating that all DoD exercises begin to include realistic cyber attacks into their war games. If this level of damage can be done by a few smart people, in a few days, using tools available to everyone, imagine what a determined, sophisticated adversary with large amounts of people, time, and money could do.

New is the wide spread knowledge of the destructive ability of cyber attacks (e.g. Aurora, Stuxnet, etc.). The cyber world has moved from exploitation and disruption to destruction.

The benefits to an attacker using cyber exploits are potentially spectacular. Should the United States find itself in a full-scale conflict with a peer adversary, attacks would be expected to include denial of service, data corruption, supply chain corruption, traitorous insiders, kinetic and related non-kinetic attacks at all altitudes from underwater to space. U.S. guns, missiles, and bombs may not fire, or may be directed against our own troops. Resupply, including food, water, ammunition, and fuel may not arrive when or where needed. Military Commanders may rapidly lose trust in the information and ability to control U.S. systems and forces. Once lost, that trust is very difficult to regain.

The impact of a destructive cyber attack on the civilian population would be even greater with no electricity, money, communications, TV, radio, or fuel (electrically pumped). In a short time, food and medicine distribution systems would be ineffective; transportation would fail or become so chaotic as to be useless. Law enforcement, medical staff, and emergency personnel capabilities could be expected to be barely functional in the short term and dysfunctional over sustained periods. If the attack's effects were reversible, damage could be limited to an impact equivalent to a power outage lasting a few days. If an attack's effects cause physical damage to control systems, pumps, engines, generators, controllers, etc., the unavailability of parts and manufacturing capacity could mean months to years are required to rebuild and reestablish basic infrastructure operation.

The DoD should expect cyber attacks to be part of all conflicts in the future, and should not expect competitors to play by our version of the rules, but instead apply their rules (e.g. using surrogates for exploitation and offense operations, sharing IP with local industries for economic gain, etc.).

[6] CJCSI 6510.01F: Information Assurance and Support to Computer Network Defense, 9 February 2011

Based upon the societal dependence on these systems, and the interdependence of the various services and capabilities, the Task Force believes that the integrated impact of a cyber attack has the potential of existential consequence. While the manifestation of a nuclear and cyber attack are very different, in the end, the existential impact to the United States is the same.

To address the widespread cyber threats, the Task Force defined cyber risk (Figure ES.2) as a function of the following parameters: threat, vulnerabilities of the systems you need to protect, and consequences of losing the systems. The threat broke into two categories: adversary intent and their capabilities. Vulnerabilities are described as either inherent or operationally introduced, and consequences either fixable or fatal to the impacted systems.

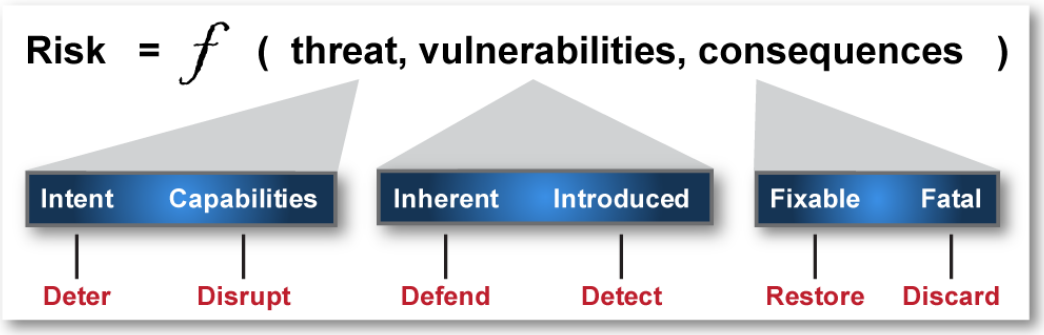

Figure ES.2 Risk Management Parameters

The Task Force could not discover a credible mechanism to reduce the value of any of the three parameters alone or in conjunction with the other parameters, to zero. Therefore, the threat, vulnerability and consequence parameters cannot be managed in isolation. A systems solution is required. Today, much of DoD's money and effort are spent trying to defend against just the inherent vulnerabilities which exist in all complex systems. Defense-only is a failed strategy.

The Task Force developed a layered approach for managing cyber risk:

- Since it will be impossible to fully defend our systems against Tier V-VI threats, deterrence must be an element of an overall risk reduction strategy.
- Defending against known vulnerabilities is an insufficient strategy against Tier III and IV threats. Additional measures are required, such as consequence management.
- When properly executed, defensive strategies can defend against Tier I and II threats.

The White House and DoD each published a cyber strategy in 2011. Both strategies note the importance of the threat and the increased diligence required to protect the country. Each strategy provides a high-level framework for a response to the cyber threat, but they lack essential details necessary to guide the DoD through execution. The Task Force believes the recommendations provided within this report offer a workable framework and fill in some of the detail about how the Department could prepare to operate in a cyber-contested environment.

The Task Force could not find a set of metrics employed by DoD or industry that would help DoD shape its investment decisions. A qualitative comparison of resources and DoD level of effort in relation to the success rate of red teams is clear evidence of the lack of useful metrics. The Task Force addresses the lack of metrics in Chapter 4 by providing a conceptual framework to put in place of metrics to improve the Department's cyber resiliency. In addition, the Task Force also proposed an initial set of performance measures that could be used to align the Department to the strategy and then measure progress toward implementation.

Recommendations

An overview of the Task Force's recommendations is included in this executive summary. Recommendation details, including proposed organizational assignments and due dates, are described further in the main body of the report.

1. Protect the Nuclear Strike as a Deterrent (for existing nuclear armed states and existential cyber attack).

- Secretary of Defense (SECDEF) assign United States Strategic Command (USSTRATCOM) the task to ensure the availability of Nuclear Command, Control and Communications (C3) and the Triad delivery platforms in the face of a full-spectrum Tier V-VI attack – including cyber (supply chain, insiders, communications, etc.).

Our nuclear deterrent is regularly evaluated for reliability and readiness. However most of the systems have not been assessed (end-to-end) against a Tier V-VI cyber attack to understand possible weak spots. A 2007 Air Force study addressed portions of this issue for the ICBM leg of the U.S. triad but was still not a complete assessment against a high-tier threat.[7]

The Task Force believes that our capacity for deterrence will remain viable into the foreseeable future, only because cyber practitioners that pose Tier V-VI level threats are limited to a few state actors who have much to hold at risk, combined with confidence in our ability to attribute an existential level attack.

2. Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary.

- SECDEF and Chairman, Joint Chiefs of Staff (CJCS) designate a mix of forces necessary for assured operation.

[7] United States Air Force Scientific Advisory Board Defending and Operating in a Contested Cyber Domain; Report on Implications of Cyber Warfare; August 2007; SAB-TR-07-02

To ensure the President has options beyond a nuclear-only response to a catastrophic cyber attack, the DoD must develop a mix of offensive cyber and high-confidence conventional capabilities. Cyber offense may provide the means to respond in-kind. The protected conventional capability should provide credible and observable kinetic effects globally. Forces supporting this capability are isolated and segmented from general purpose forces to maintain the highest level of cyber resiliency at an affordable cost. Nuclear weapons would remain the ultimate response and anchor the deterrence ladder. This strategy builds a real ladder of capabilities and alleviates the need to protect all of our systems to the highest level requirements, which is unaffordable for the nation. Similar to the prior argument regarding the cyber resiliency of the nuclear deterrent, DoD must ensure that some portion of its conventional capability is able to provide assured operations for theater and regional operations within a full-spectrum, cyber-stressed environment.

Because of the expected cost of implementation, the protected-conventional capability must support a limited number of cyber critical survivable missions. This Task Force recommends improving the cyber resiliency of a mix of the following systems for assured operation in the face of a full spectrum adversary: global selective strike systems e.g. penetrating bombers, submarines with long range cruise missiles, Conventional Prompt Global Strike (CPGS),[8] survivable national and combatant command (CCMD) C2.

- Segment Sufficient Forces to Assure Mission Execution in a Cyber Environment

Segmentation must differentiate only sufficient forces required to assure mission execution; it is not required across an entire capability. For example, if long range strike is a component of the protected-conventional capability, then DoD should segment a sufficient quantity that is designated as a cyber critical survivable mission. Notionally, 20 aircraft designated by tail number, out of a fleet of hundreds, might be segregated and treated as part of the cyber critical survivable mission force. Segmented forces must remain separate and isolated from the general purpose forces, with no dual purpose missions (e.g. the current B-52 conventional/nuclear mission).

DoD must engage multi-agency counterparts for an updated Strategic Deterrence Strategy, including the development of cyber escalation scenarios and thin lines.

3. Refocus Intelligence Collection and Analysis to Understand Adversarial Cyber Capabilities, Plans and Intentions, and to Enable Counterstrategies.

[8] DSB Task Force on Time Critical Conventional Strike from Strategic Standoff, March 2009

- SECDEF in coordination with the Directors of CIA, FBI, and DHS, should require the Director of National Intelligence (DNI) to support enhanced intelligence collection and analysis on high-end cyber threats.

Intelligence must include the identification and understanding of adversarial cyber weapon development organizations, tools, leadership, and intentions, and the development of targeting information to support initiatives to counter cyber weaponization. Mitigating a Tier V-VI threat is impossible without filling these intelligence gaps. Therefore, the Intelligence Community (IC) should increase the priority of its intelligence collection and reporting requirements in this domain.

4. Build and Maintain World-Class Cyber Offensive Capabilities (with appropriate authorities).

- United States Cyber Command (USCYBERCOM) develop capability to model, game and train for full-scale cyber warfare.
- Under Secretary of Defense for Personnel and Readiness (USD(P&R)) establish a formal career path for civilian and military personnel engaged in offensive cyber actions.

Today, the United States is a leader in cyber offensive capabilities. However, most training and engagements are very limited and in controlled environments. Preparing for full-scale force-on-force cyber battle is not well understood. Challenges range from the scale of numbers of expected sorties to uncertainty of triggering mechanisms, trust and capability recovery timelines, and potential blowback of attacks all happening within the fog of war. To prepare, DoD must first begin to understand the full complexities of cyber war.

Recommendations include developing the capability to model, war game, red team and eventually train for full scale peer-on-peer cyber warfare. A policy framework should be established for offensive cyber actions, to include who has the authority and under what circumstances and controls to act.

Finally, DoD needs to significantly increase the number of qualified “cyber warriors” and enlarge the offensive cyber infrastructure commensurate with the size of threat. Professionalizing the cyber offense skill set and providing career ladders in this new field will be a key element toward growing the human resources required to compete effectively. This report is especially concerned with developing top-tier talent who can be certified to perform at the elite or extreme cyber conflict levels. The United States needs such world class performers in substantial numbers--some of whom may not be eligible for security clearances.

5. Enhance Defenses to Protect Against Low and Mid-Tier Threats.

- DoD Chief Information Officer (CIO) in collaboration with the Military Departments and Agencies establish an enterprise security architecture, including

appropriate "Building Codes and Standards", that ensure the availability of enabling enterprise missions.

Some adversaries will not be deterred (e.g., terrorist organizations and lone wolves); DoD must defend its systems against these low- and mid-tier threats. Therefore, the Task Force recommends that the DoD CIO establish a DoD-wide "Enterprise" architecture, including "building codes and standards" that ensure availability of mission operations during peace-time and full-spectrum wartime events. The building code analogy suggests that DoD should not make every network across the DoD identical, but instead should ensure that all networks, even when tailored by the Military Departments and end-users, meet a robust set of minimum standards that ensure a reasonable system network defense can be provided. U.S. networks also need requirements for instrumentation to increase the probability of detection of attacks and create situational awareness to speed remediation. Existing acquisition programs should be influenced, to the maximum extent feasible, with the new requirements. Audits should be conducted to the standard, and conducting in-process reviews to develop migration and mitigation strategies are critical. Legacy systems that cannot be maintained in a timely manner, (and DoD has many of them) must be enclaved and firewalled from the Global Information Grid (GIG).

Commercial technologies that enable the automation of some network maintenance activities and provide real-time mitigation of detected malware are available today. The Task Force believes that use of these technologies would actually drive network operation costs down and free up resources to hunt on the network for intruders.

6. Change DoD's Culture Regarding Cyber and Cyber Security.

- SECDEF/CJCS establish a DoD-wide policy, communication, education and enforcement program to change the culture regarding cyber and cyber security

Establish a DoD-wide policy, communication, and education program to change the cyber culture. When focused, DoD can be one of the most disciplined large organizations in the world. It is this discipline that enables DoD to establish and execute processes that ensure the physical fitness of the armed forces, the safe and secure handling of weapons and the effective management of classified material. The same level of importance and discipline has not been applied to cyber hygiene and security. We will not succeed in securing our systems against even low- and mid-tier threats without changing this dynamic.

Communication of the critical importance of DoD cyber hygiene must be led by the SECDEF, CJCS, and their direct reports. Updated policies and training programs, and providing clear, punitive consequences for breach of policy will be necessary to move DoD to a higher level of cyber readiness.

7. Build a Cyber Resilient Force.

- Deputy Secretary of Defense (DEPSECDEF) should direct specific actions to introduce cyber resiliency requirements throughout DoD force structure to include:

- Build a set of standards/requirements that incorporate cyber resiliency into the cyber critical survivable mission systems identified in Recommendation 2, (Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), DoD CIO)

The DoD CIO, in coordination with USD(AT&L), should establish a resiliency standard to design, build and measure capability against. The Joint Staff will use the standard to inform the requirements process. The cyber resiliency standard should be applied to sufficient segments of the force structure identified as the conventional components of the escalation ladder (see Recommendation 2) to achieve a credible deterrent effect.

- Apply a subset of the cyber resiliency standard developed above to all other DoD programs (USD(AT&L), DOD CIO, Service Acquisition Executives (SAEs))
- Increase feedback from testing, red teaming, the Intelligence Community, and modeling and simulation as a development mechanism to build-out DoD's cyber resilient force (USD(AT&L), Undersecretary of Defense for Intelligence (USD(I)), DOT&E, SAEs, CJCS)
- Develop a DoD-wide cyber technical workforce to support the build out of the cyber critical survivable mission capability and rollout to DoD force structure (USD(AT&L), CIO, SAEs, Director, Operational Test and Evaluation (DOT&E), USD(I), USD(P&R))
- Science and Technology community establish secure system design project with Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), academia, commercial and defense industry (Assistant Secretary of Defense for Research and Engineering (ASD(R&E))
- Intelligence community should initiate a supply chain collection activity (USD(I))

Investment Requirements

While it is difficult to project investment costs within an organization as broad and diverse as the DoD, the Task Force attempted to predict the ranges of cost and approximate time frames for which these recommendations could be accomplished, as shown in Table ES.1

Table ES.1 Estimated Investment Requirements for Study Recommendations

		ROM	Timeframe
1 & 2	Protect the Nuclear Strike as a Deterrent (for existing nuclear armed states and existential cyber attack). Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary.	$$$$	36-60 mo.
3	Refocus Intelligence Collection and Analysis to Understand Adversarial Cyber Capabilities, Plans and Intentions, and to Enable Counterstrategies.	$	12-24 mo.
4	Build and Maintain World-Class Cyber Offensive Capabilities (with appropriate authorities).	$$	12-24 mo.
5	Enhance Defenses to Protect Against Low and Mid-Tier Threats.	$	6-18 mo.
6	Change DoD's Culture Regarding Cyber and Cyber Security.	$	12-48 mo.
7	Build a Cyber Resilient Force.	$$	12-24 mo.
ROM Costs $ <$50M/yr, $$ $50M-$100M/yr, $$$ $100M-$500M/yr, $$$$ >$500M/yr			

The good news is, even within the difficult current budget environment, much can be done to address challenges faced in the cyber domain. The Task Force believes the Department must move quickly to better understand the interrelationship between the cyber threat, national defense, and deterrence. The only recommendations requiring a large amount of resources are that of ensuring the strategic deterrent is protected to a high degree of confidence, and building a protected set of conventional capabilities. While the basic components of these systems exist today, understanding their cyber vulnerabilities, and separating their C2 systems, providing backup or war reserve capabilities to ensure available operation, will require time and resources.

Measuring Progress

The Task Force unsuccessfully searched for cyber metrics in commercial, academic, and government spaces that directly determine or predict the cyber security or resilience of a given system--which could ultimately be used by the Department to manage and shape its cyber investments. Instead, the Task Force provided an implementation plan to develop the measurement systems to help the Department execute the strategy defined within this report and then measure performance within that structure. If the Department chooses a different path, the implementation plan can be tailored to address alternate choices. Fundamentally, any metrics based approach must establish a mechanism to determine what will be measured, develop an appropriate collection system and construct appropriate performance measurements.

In any enterprise, metrics are only successful if their application is driven from the top leadership down through the organization, and followed up with consistent, determined attention. The measures recommended herein serve as a starting point for the Department, but ultimately, experience shows that in any enterprise, metrics will develop and evolve over time

as experience is gained. This may seem like a trivial action, but from an historical and cultural aspect, this would be very new to the DoD.

The proposed framework enables leadership to first monitor the establishment of the collection systems, processes and activity created to implement the Task Force recommendations. Figure ES.3 below shows the first of two proposed metric panels, identifying the establishment of the metric collection systems to implement the Task Force recommendations. Within each recommendation (deterrent, intelligence, world-class offense…), a series of steps, from least to most complicated, are defined with the objective to track the systematic development of enterprise cyber resiliency capability. A maturity level approach is used to ensure the Department can prepare a solid foundation for achieving cyber resilience and allow flexibility if the Department chooses alternative paths to achieving cyber resiliency.

At a minimum, each component of the metric collection system in Figure ES.3 must define a common language and standards that can be used across the enterprise and identify reporting and tracking mechanisms that allow leadership the ability to track progress toward the intended goal. Without a common language, any effort will probably fail due to the inability to compare performance across the enterprise. For example, if the Department immediately leapt to an automated intrusion detection collection system without knowing the components of each separate network, or understanding how to detect an intrusion, or how to identify which network architectures supported automation, or when intrusions should be reported, etc. then comparing collected data would involve significant amounts of work just to ensure Network A is looked at the same way as Network Z.

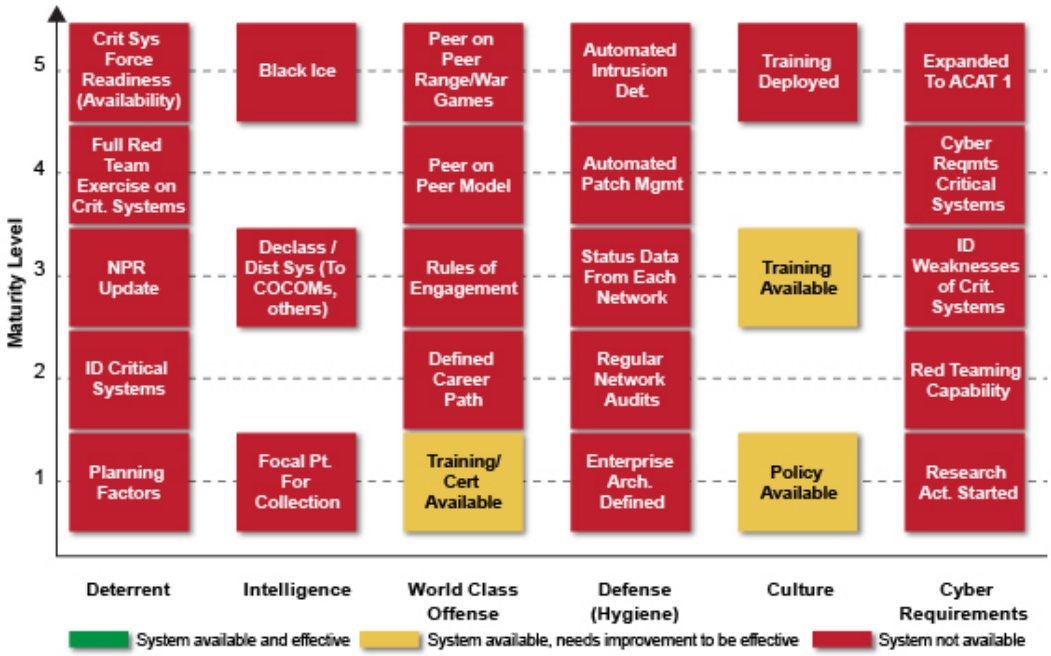

Figure ES.3 Notional Dashboard – Metric Collection System

Once the metric collection systems are identified and in place, performance metrics can be defined to give the Department an understanding of its cyber readiness (Figure ES.4). When properly defined, performance measures provide better insight into actual status. Accurate information gathered from the bottom up can be used to tie the data to expenditures and enable visibility into the actual costs of managing network elements. For example, a set of defense/cyber hygiene performance metrics start with a simple count of audits. A line manager could look at the graph and tell immediately how much of the network was audited and the results of the audit. Since definitions are common across the enterprise, upper level managers are alerted to danger areas when too many audits result in failure. Audits also expose network components because properly conducted audits require a high fidelity inventory of network components. This creates an ability to measure the cost to manage network elements. Other performance metrics identify the time to patch a system and the time to detect an intruder once a vulnerability is identified.

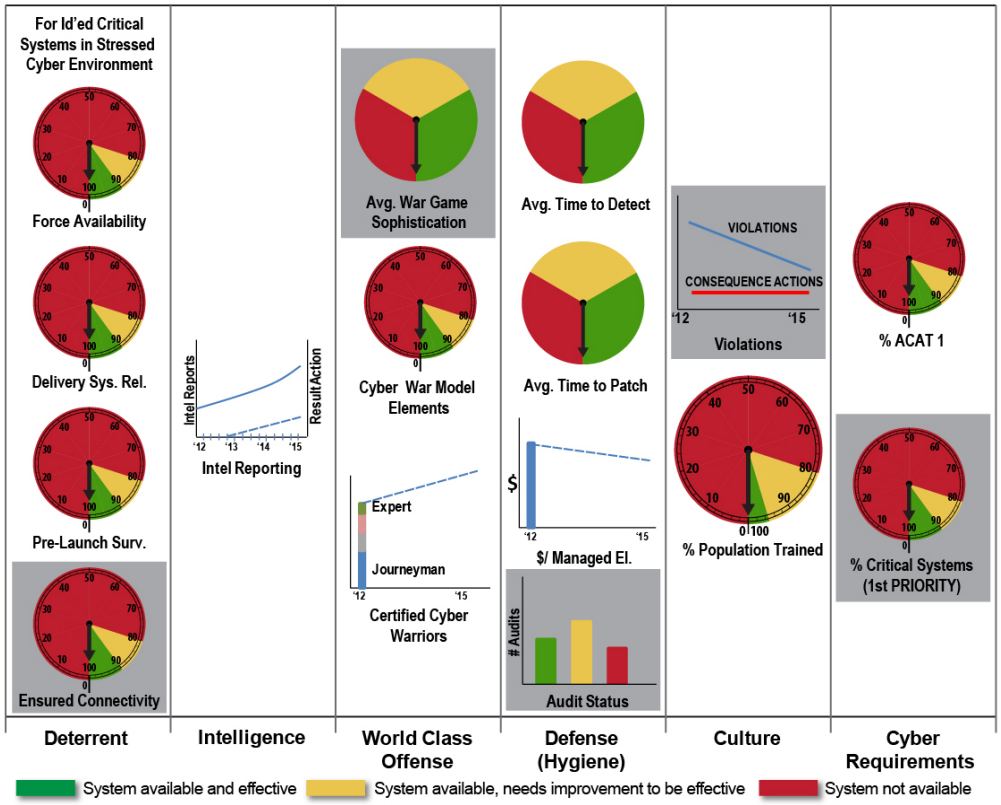

Figure ES.4 Notional Dashboard – Performance Metrics

Ultimately, performance metrics identify best practices that can then be shared across the organization. Peer pressure between network owners will encourage improved performance by those responsible.

The Department will do best to measure outcomes, such as the average time it takes to detect a successful attack that breaches the network perimeter defenses, and the amount of time it takes to recover a system that is lost as a result of a cyber attack. Little value would be

generated by jumping to outcome metrics without the common enterprise standards, audit definitions, and an understanding of what the metrics mean. The Task Force estimates that the DoD would have an experience base within two years of gathering data that would begin to allow comparisons of architectures, networks, and system elements for their cyber resilience and cost to operate. That data would provide DoD insight to inform predictions of performance of various architectures and elements versus available budgets. However, the Department must be disciplined and thoughtful about its use of metrics. Poorly defined and improperly used metrics may prove as harmful as no metrics at all.

Conclusion

The network connectivity that the United States has used to tremendous advantage, economically and militarily, over the past 20 years has made the country more vulnerable than ever to cyber attacks. At the same time, our adversaries are far more capable of conducting such attacks. The DoD should expect cyber to be part of all future conflicts, especially against near-peer and peer adversaries. This Task Force believes that full manifestation of the cyber threat could even produce existential consequences to the United States, particularly with respect to critical infrastructure. To maintain global stability in the emerging area of cyber warfare, the United States must be, and be seen as, a worthy competitor in this domain.

This Task Force developed a set of recommendations that, when taken in whole, creates a strategy for DoD to address this broad and pervasive threat. Cyber is a complicated domain and must be managed from a systems perspective. There is no silver bullet that will reduce DoD cyber risk to zero. While the problem cannot be eliminated, it can and must be determinedly managed through the combination of deterrence and improved cyber defense. Deterrence is achieved with offensive cyber, some protected-conventional capabilities, and anchored with U.S. nuclear weapons. This strategy removes the requirement to protect all of our military systems from the most advanced cyber threats, which the Task Force believes is neither feasible nor affordable. It will take time to build the capabilities necessary to prepare and protect our country from the cyber threat. **We must start now!**

1.0 Introduction

1.1 Identification of This Report

This document (and its companion appendices) constitutes the final report of the Defense Science Board (DSB) Task Force study on Resilient Military Systems. This effort was one component of the DSB Cyber Initiative. The other component is addressed by the DSB Task Force on Cyber Security and Reliability in a Digital Cloud. This report is the culmination of a year-plus study by a Task Force comprised of over 20 topic-knowledgeable members selected from the private sector. (See Appendix 2 for a listing of the Task Force membership and structure.)

As described in Appendix 3, the Task Force received briefings from civilian, military and private sector personnel from across the spectrum of research, development, acquisition, administration, operation, and use of automated systems.

1.2 Study Purpose

The DSB study on Resilient Military Systems and the Advanced Cyber Threat was commissioned by the Deputy Secretary of Defense, the Hon. William J. Lynn, on May 19, 2011 to:

- Study, and if possible, define meaningful measures and metrics to evaluate and monitor the level of DoD operational system resiliency in the face of a cyber attack.
- Identify strategies and techniques that could improve DoD system resiliency in the face of a cyber attack.

The study Terms of Reference (TOR) (Appendix 1) focused on maintaining the global ability to defend the Nation in the face of increasingly sophisticated and potentially devastating, cyber exploitation and attack. Some portions of the TOR are repeated below for clarity and emphasis.

Recognizing that the superiority of U.S. military systems is critically dependent upon increasingly vulnerable information technology, the Department requested assistance from the DSB in seeking a new perspective on the ways it manages and defends military systems against cyber exploitation and attack.

> **"Innovative use of modern information and communications technology (ICT) (e.g. networks, software and microelectronics) in military systems plays a key and vital role in making the U.S. military second to none. However, the effectiveness of these military systems is extremely dependent upon the information assurance provided by its ICT underpinnings and of the personnel who operate and maintain the systems. An unintended consequence of the reliance on ICT to sustain superior U.S. capability is that our adversaries can erode or eliminate our advantage by targeting and exploitation at both the system and component level."**
>
> **"…To continue to take advantage of modern technology to increase our military effectiveness, we must possess sufficient confidence that these systems are not compromised to such a degree that we lose the benefit. In addition, we want to actively decrease the confidence of our adversaries that their clandestine operations targeting our systems would be effective enough to eliminate our advantage."**

The challenges of mounting an effective cyber defense are well-appreciated by the Department's civilian and military leaders. However, the continually evolving environment of cyber threat and increasing system vulnerabilities poses a worsening situation that demands a more comprehensive and pro-active risk management approach. Effective management entails the ability to measure the relative strengths and weaknesses of cyber capabilities as well as organizational progress toward improvement implementation.

> **"…Based in part on the complexity of modern software and microelectronic systems, very small and difficult to detect defects or subversive modifications introduced at some point in the life cycle of the systems can create debilitating effects…As a result of the great and growing complexity of DoD systems, cyber resiliency is an extremely broad and difficult attribute to guarantee."**

> **"…An important step toward designing, implementing and maintaining more resilient systems is to understand how to effectively measure the resiliency of those systems relative to various cyber attacks and adversaries…[to ensure that] they will perform as expected in a hostile environment."**

Recognizing the importance of effective measures or metrics and the difficulty in creating good metrics, the DSB was asked to seek any such cyber-relevant measures currently in use as well as to suggest areas where useful metrics might be developed.

1.3 Study Background and Special Circumstances

For the past three decades, the United States has led the world in developing and leveraging networks and embedded cyber capabilities to build a significant advantage across a number of linked National Security areas (e.g. military capabilities, intelligence, and the defense industrial base). The resulting DoD doctrine (Joint Vision 2010, 2020) of Full Spectrum Dominance envisioned information superiority to great advantage as a force multiplier. The power of this doctrine and its near total reliance on information superiority led to networking almost every conceivable component within DoD, with frequent networking across the rest of Government, commercial and private entities, and coalition partners in complex, intertwined paths. While proving incredibly beneficial, these ubiquitous IT capabilities have also made the United States increasingly dependent upon safe, secure access and the integrity of the data contained in the networks. A weakness of the implementation of this doctrine is its focus on functionality, connectivity and cost of information superiority over security--similar to the development of the Internet.

The performance of U.S. military forces over the last decade has demonstrated the superiority of networked systems coupled with kinetic capabilities and well-trained forces. While it is doubtful that the United States will face a peer force in the immediate future, "our" adversaries have discovered that the same connectivity and automation that provides great advantage to the US, is also a weakness that presents an opportunity to undermine U.S. capabilities in a very asymmetric way. The same network attack tools that are available on the commercial market are available to our adversaries. In addition, adversaries with financial means will invest to improve those tools and build more capable weapons to attack U.S. military systems and

national infrastructure. Recent reports of Iran building cyber capabilities and Al Qaeda video releases with how-to instructions encouraging attacks on U.S. infrastructure are troubling.

In addition to state sponsored attacks against U.S. military capability, a wide range of actors (e.g. criminals, state sponsored economic espionage, etc.) employ cyber tools to pursue illicit economic gain. The almost daily release of new press reports and studies describe the risk and economic harm created by constant cyber attacks against commercial (e.g. financial, social, e-mail, etc.) and government systems. Symantec reports blocking over 5.5 billion attacks with its software in 2011 alone finding that the average breach exposed 1.1 million identities and nearly 5,000 new vulnerabilities were identified in the calendar year.[9] Over 400 million unique variants of malware attempted to take advantage of those vulnerabilities, up 40% from 2010. Attack toolkits are easy to find and available in web forums or on the underground black-market and cost only $40-$4,000 to procure. Use of these widely-available tools allows almost anyone to exploit any known and uncorrected vulnerability.

Over the last several years, concern over America's cyber risk has made regular headlines and has been the subject of many studies. In January 2008, President Bush launched the Comprehensive National Cyber Security Initiative. In May 2009, President Obama accepted the recommendations of the Cyberspace Policy Review to ensure an organized and unified response to future cyber incidents; strengthen public/private partnerships to find technology solutions that ensure U.S. security and prosperity; invest in the cutting-edge research and development necessary for the innovation and discovery to meet the digital challenges of our time; begin a campaign to promote cyber security awareness and digital literacy from our boardrooms to our classrooms; and begin to build the digital workforce of the 21st century. With the establishment of various cyber initiatives and strategies, the standing-up of USCYBERCOM, and the development of greater cyber capabilities within the DoD Military Departments and our Nation's intelligence agencies, the United States is moving in the right direction. However, to date, this increased activity lacks coordination and consistent strategic intent.

This is not the first time the DSB has addressed the subject of cyber security. Indeed, the DSB has repeatedly warned of increasing vulnerabilities of information and communication technologies, the growing cyber threat from state actors as well as smaller groups, and the lack of adequate priorities placed on cyber matters by Department management (Table 1.2 Previous DSB Studies That Have Addressed the Cyber Theme).

[9] Internet Security Threat Report, Volume 17; 2011; Symantec

Table 1.2 Previous DSB Studies That Have Addressed the Cyber Theme

February 2011	2010 Summer Study on Enhancing Adaptability of our Military Forces
September 2007	Mission Impact of Foreign Influence on DoD Software
April 2007	2006 Summer Study on Information Management for Net-Centric Operations, Volume I
April 2007	2006 Summer Study on Information Management for Net-Centric Operations, Volume II
January 2007	Critical Homeland Infrastructure Protection
February 2005	High Performance Microchip Supply
June 2001	Defensive Information Operations, Vol. II, Part 2
March 2001	Defensive Information Operations, Vol. II
February 2001	2000 Summer Study on Protecting the Homeland: Report on Defensive Information Operations
November 1996	Information Warfare Defense
October 1994	1994 Summer Study on Information Architecture for the Battlefield

The topic of cyber exploitation and attack has been openly addressed in public policy as well as in the press, and the tempo is escalating. Due to the sensitive nature of facts and background data related to cyber, versions of this report were prepared at appropriate classification levels.

1.4 Working Terminology, Scope, and Definitions for this Study

For the purposes of this DSB study, the term **Cyber** is broadly used to address all digital automation used by the Department and its industrial base. This includes weapons systems and their platforms; command, control, and communications systems; intelligence, surveillance, and reconnaissance systems; logistics and human resource systems; and mobile as well as fixed-infrastructure systems. "Cyber" applies to, but is not limited to, "IT" and the "backbone network," and it includes any software or applications resident on or operating within any DoD system environment. (See Appendix 4 for a more complete listing of acronyms used in this report.)

Cyber encompasses the entirety of digital electronic systems and devices used by DoD. In today's world of hyper-connectivity and automation, any device with electronic processing, storage, or software is a potential attack point and every system is a potential victim–including our own weapons systems. Cyber is not the exclusive purview of USCYBERCOM, the DoD Chief Information Officer (CIO), the Defense Information Systems Agency (DISA), or the individual system support activities of the Military Departments and Commands. Neither can it be discounted by resource planners or system research, development, and acquisition authorities as somehow beyond their responsibilities. Cyber provides an area of common concern for all these organizations (and more) – an area where all must work together in addressing this rapidly emerging threat.

Resilience is the ability to continue or return to normal operations in the event of some disruption: natural or man-made, inadvertent or deliberate. A goal of DoD is to have **mission resiliency** in the face of all forms of failure (including espionage and attack). Thus, commanders must develop alternative mission plans, emergency procedures, and reinforcements and re-supply options. Similarly, for **cyber system resiliency** there must be alternative system plans, emergency back-up procedures, and reconfiguration/restart options. In modern warfare, effective mission resiliency requires that all systems critical to mission accomplishment be resilient.

In this study, the Task Force deliberately viewed DoD as a globally networked enterprise – a complex entity of highly interconnected and interdependent components, each of which may contain embedded cyber capabilities-where failure to accomplish a mission can have far-reaching impact with potentially serious national security consequences. Because of the nature of cyber exploitation and attack, failure to protect the enterprise at any possible point of entry can expose the entire enterprise to potentially devastating results.

1.5 Report Structure

This report is laid out as follows. Following this Introduction, Chapter 2 provides an explanation of the growing cyber threat to our military mission. Chapter 3 offers a comprehensive strategic approach for addressing system resiliency in the face of the ongoing cyber threat, and Chapter 4 addresses approaches to measuring progress in implementing the strategy. Chapters 5 through 10 address key aspects of the strategy, namely: ensuring deterrence through our nuclear and conventional military strike capability, collecting intelligence on peer adversaries' cyber capabilities, developing broader cyber offensive capabilities available to the United States, enhancing the U.S. military's cyber defense to thwart low- and mid-tier threats, changing DoD's cyber culture to take security more seriously, and building a cyber-resilient force. Chapter 11 provides order of magnitude cost estimates for implementing the proposed strategy. Chapter 12 provides a summary of the study conclusions and recommendations. The document concludes with a series of appendices containing ancillary, technically detailed and/or classified information.

In this study, the Task Force did not examine policies and authorities related to rules of engagement, use of cyber offensive capabilities, and inter-agency issues such as the protection of civilian infrastructure. These, nevertheless, are also crucial to the DoD.

2.0 Understanding the Cyber Threat

U.S. military forces are critically dependent on networks and information systems to execute missions. They are thus highly vulnerable if threats to those networks and information systems are not sufficiently addressed. This chapter describes that threat – first, by defining it; then discussing its realization; and finally considering the impacts of this realization.

2.1 Definition of the Cyber Threat

The cyber threat is characterized in terms of three classes of increasing sophistication: those practitioners who rely on others to develop the malicious code, those who can develop their own tools to exploit publically known vulnerabilities as well as discovering new vulnerabilities, and those who have significant resources and can dedicate them to creating vulnerabilities in systems. The definition adopted by the Task Force enables a more detailed discussion of the characteristics of threat actors, mechanisms that can be used to protect or harden cyberspace components and operations dependent on those components, the impacts that threat actors pose if they are successful in their malevolent behavior, and recovery or response actions commensurate with the specific threat actions.

The taxonomy developed by the Task Force is summarized in Figure 2.1 Cyber Threat Taxonomy. As shown, the threat is divided into three levels of increasing sophistication, each composed of two tiers.

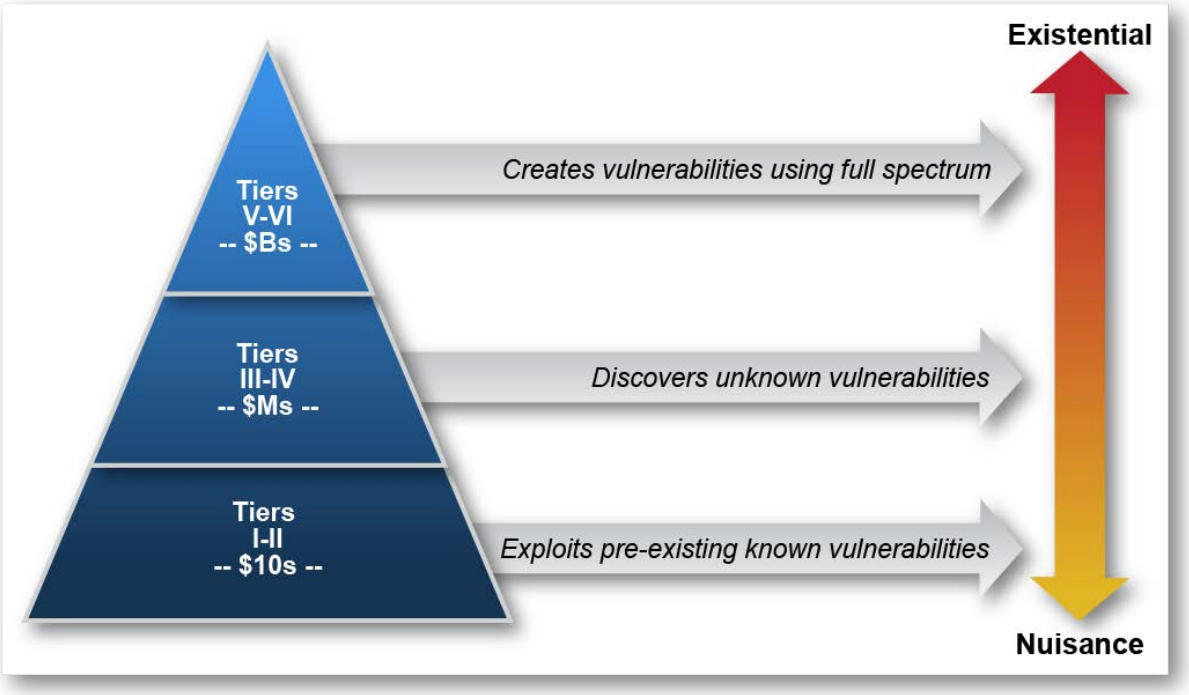

Figure 2.1 Cyber Threat Taxonomy

Dollar figures specified for each tier indicate the nominal investment required to participate at the given tier. The width of the figure at the given tiers suggests the decreasing number of practitioners as one ascends the pyramid to higher tiers. There are a vast number of parties with Tier I and II capabilities, while only a few state actors possess Tier V and VI capabilities.

Table 2.1 provides definitions of the tiers. Tier I practitioners, using malicious code developed by others, are commonly referred to as "script kiddies" and are driven as much by the desire to brag about their success in executing an "attack" as they are to cause specific damage. Tier II actors have some ability to develop their own malicious code and their actions may be characterized by pursuit of specific objectives such as the theft of business or financial data. Low-tier actors can employ some very sophisticated tools and techniques developed and exposed by others. Tier III and IV actors employ a broad range of software capabilities to penetrate cyber systems and effect exploits through Internet access. A major distinction between Tiers III and IV is scale – Tier IV is characterized by larger, well-organized teams, either state or criminal. Tiers V and VI encompass actors who can go beyond malicious software inserted through Internet access, and instead, create vulnerabilities in otherwise well-protected systems. Tier V actors are able to insert malicious software or modified hardware into computer and network systems at various points during their lifecycle for later exploit (e.g., a "cyber time bomb"). Tier VI organizations employ full-spectrum techniques, including humans (e.g., spies engaged in bribery and blackmail) and close-access means (physical or electronic) to gain system penetration, and have the resources to conduct many operations concurrently.

Table 2.1 Description of Threat Tiers

Tier	Description
I	Practitioners who rely on others to develop the malicious code, delivery mechanisms, and execution strategy (use known exploits).
II	Practitioners with a greater depth of experience, with the ability to develop their own tools (from publically known vulnerabilities).
III	Practitioners who focus on the discovery and use of unknown malicious code, are adept at installing user and kernel mode root kits[10], frequently use data mining tools, target corporate executives and key users (government and industry) for the purpose of stealing personal and corporate data with the expressed purpose of selling the information to other criminal elements.
IV	Criminal or state actors who are organized, highly technical, proficient, well funded professionals working in teams to discover new vulnerabilities and develop exploits.
V	State actors who create vulnerabilities through an active program to "influence" commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest.

[10] User mode rootkits involve system hooking in the user or application space. Whenever an application makes a system call, the execution of that system call follows a predetermined path and a Windows rootkit can hijack the system call at many points along that path. Kernel mode rootkits involve system hooking or modification in kernel space. Kernel space is generally off-limits to standard authorized (or unauthorized) users. One must have the appropriate rights in order to view or modify kernel memory. The kernel is an ideal place for system hooking because it is at the lowest level and thus, is the most reliable and robust method of system hooking.

Tier	Description
VI	States with the ability to successfully execute full spectrum (cyber capabilities in combination with all of their military and intelligence capabilities) operations to achieve a specific outcome in political, military, economic, etc. domains and apply at scale.

Three comments about higher-tier actors should be made. First, while capable of operating at the higher levels, higher-tier actors will use the methods and techniques at the lowest level necessary to accomplish their objectives. They "hide" in the larger set of activity at lower levels to avoid exposing their more sophisticated techniques. Second, states might employ non-state actors as proxies. In such situations, middle-tier organizations gain access to higher-tier capabilities. This is especially true in states that are not as aggressive (passionate) as the United States is about separating the state from commercial and social society, which then blurs distinctions that this Task Force adopted. Third, the scale at which an organization can operate is one of the major discriminators between Tiers V and VI. Operations at scale is particularly challenging at Tier VI because of the complexity and potentially long times required to effect an operation using full-spectrum methods. While one might argue that "most any target" could be penetrated using Tier VI methods and sufficient time, to do so is expensive and resource intensive. The discriminator of a Tier VI actor is funding, people and equipment to conduct many such operations concurrently.

The following examples illustrate the threat-hierarchy tiers. Phishing, wherein malicious code is contained in an email from an unknown source, is an example of a Tier I threat. Spear-phishing, wherein malicious code is contained in an email attachment supposedly from a known party, is an example of a Tier II threat. The most sophisticated Spear-phishing attacks will impersonate a highly trusted source (e.g. close friend, co-worker, boss, etc), and less-sophisticated attacks use broader relationships as the known source (e.g. social network, organization, etc). The recently disclosed Flame virus[11] is an example of a Tier IV threat. It is highly complex software and most likely required a well-funded professional team to develop it. The software complexity and sophistication of OPERATION BUCKSHOT YANKEE[12] are those of Tier IV.

Examples of a Tier V-VI threat include hardware modifications followed by insertion of the hardware into a target system. A recently declassified example of a [then] high-tier exploitation is a Soviet Union operation against the United States during the Cold War designated by the United States as Project GUNMAN.[13] In the 1970s and early '80s, the IBM Selectric typewriter was considered an advanced electromechanical "computer" of its day. Soviet "cyber warriors" managed to replace the comb support bar (Figure 2.2) of the typewriter with a device that externally looked the same but was cleverly modified to enable the transmission in plain text of

[11] "Cyberattacks on Iran—Stuxnet and Flame;" New York Times; June 1, 2012

[12] OPERATION BUCKSHOT YANKEE is the code name of the Pentagon's operation to counter the attack that then Deputy Secretary Lynn described in his 2010 Foreign Affairs article cited in this report's Executive Summary

[13] Maneki, Sharon; "Learning from the Enemy: The Gunman Project;" Center for Cryptologic History, National Security Agency; 2009

nearly every typed key to a nearby Soviet listening post. Between 1976 and 1984, sixteen of these typewriters found their way into the U.S. Embassy in Moscow and the U.S. Mission in Leningrad.

The level of sophistication employed by the Soviets made U.S. discovery unlikely without a tipoff from a liaison service exposed to a similar attack. Technical modifications included integrated circuit design technology never before seen by National Security Agency (NSA) engineers, burst transmission techniques designed to defeat U.S. technical security countermeasure equipment, and designs that employed parts of the typewriter as an antenna to transmit the information and provide power, and finally, foretelling later awareness of the field of human factors engineering, a design that allowed easy insertion and maintenance of the modified equipment. Additional non-technical exploitations included Soviet use of unfettered access permitted at customs checkpoints to insert the devices and hiding in the noise of its traditional technical espionage techniques. The Soviets had a longstanding proclivity to employ audio devices against the U.S. Embassy and diplomatic missions that created a U.S. mindset that assumed the Soviets only employed audio devices (e.g. the new U.S. Moscow embassy that began construction in 1979 was so riddled with implanted listening devices that the United States eventually rejected the building). Even after the tipoff from the liaison service, the U.S. effort to recover the modified equipment and discover the vulnerability required several months. Discovering the modification required an NSA team of approximately 25 engineers working six days a week and the use of X-ray techniques. Even though integrated circuits were relatively simple compared to today's designs, the NSA engineers initially debated whether the anomaly discovered by X-rays was caused by a Soviet modification or was caused by IBM introducing memory circuits into the Selectric. Once the location of the modification was discovered, reverse engineering took additional time and resources to discover how the device worked.

Figure 2.2 Example of a Cold-War era Tier VI Cyber Exploitation

The complexity of modern integrated circuit processors makes a modern version of the GUNMAN Tier VI capability very feasible (Figure 2.3). Removal of an integrated circuit from its packaging and replacement with a subversive die into the same package can be used to modify processor behavior under trigger conditions determined by the attacker.

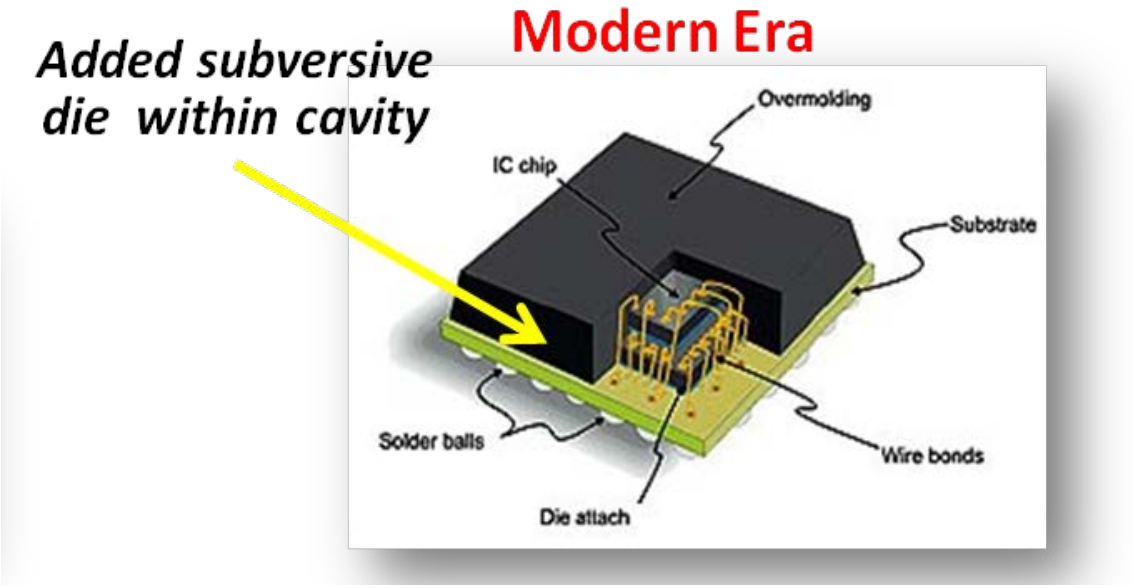

Figure 2.3 A Notional Modified Integrated Circuit

The subversive die would not affect system performance through testing qualification or operation until a triggering mechanism was activated (e.g. the reading of specific input by the chip, geographic coordinates or aircraft velocity value, or through external connectivity like software patching mechanisms). This would make it very difficult to find the compromised chip in our systems through inspection or operation - just as it was in the Gunman operation. This chip could be inserted into a specific system through surreptitious means or inserted into a larger batch of systems during "normal" manufacturing in some foreign nation. The subversive die's effects could destroy the processor and disable the system by simply shunting power to ground, change the processor output to incorrect results for specified inputs, or allow information leakage to the attackers. To address the seriousness of the threat, DoD launched a number of supply chain initiatives, including the Trusted Foundry Program in 2004 to help ensure the integrity of hardware and software components in its critical systems.

2.2 Impact of the Cyber Threat

Many factors make modern computing and networking systems vulnerable to the above threats – for example:

- The original Internet design precepts that presumed trusted users, and promised a high degree of user anonymity, yielded an inherently vulnerable system with barriers to attribution

- The complexity of modern software and hardware makes it difficult, if not impossible to develop components without flaws or to detect malicious insertions
- Many building blocks are created and maintained by third-party sources (e.g. open-source)
- The widespread use of commercial software and hardware (COTS) produced for markets that have low concerns about security
- The offshore development of software and hardware by parties of unknown trust

Figure 2.4 and Figure 2.5 illustrate the complexity issue. The source lines of code (SLOC) of commercial operating systems have grown to nearly 50 million. Government programs depict similar growth trends over several decades.[14,15] On the hardware side, complex integrated circuits now have over 2 billion transistors. It is impossible to comprehensively test such software (anybody who uses a software product is very familiar with the concept of software updates) and hardware products (the Pentium floating point flaw discovered in 1994 shortly after the processor went to market is an example) completely for vulnerabilities.[16] Attempting to fully test systems of these complexities would take years per operating system or device using state of the art equipment. In addition, the design, development and production processes are highly automated and dispersed, relying on libraries for hardware functions and source code.

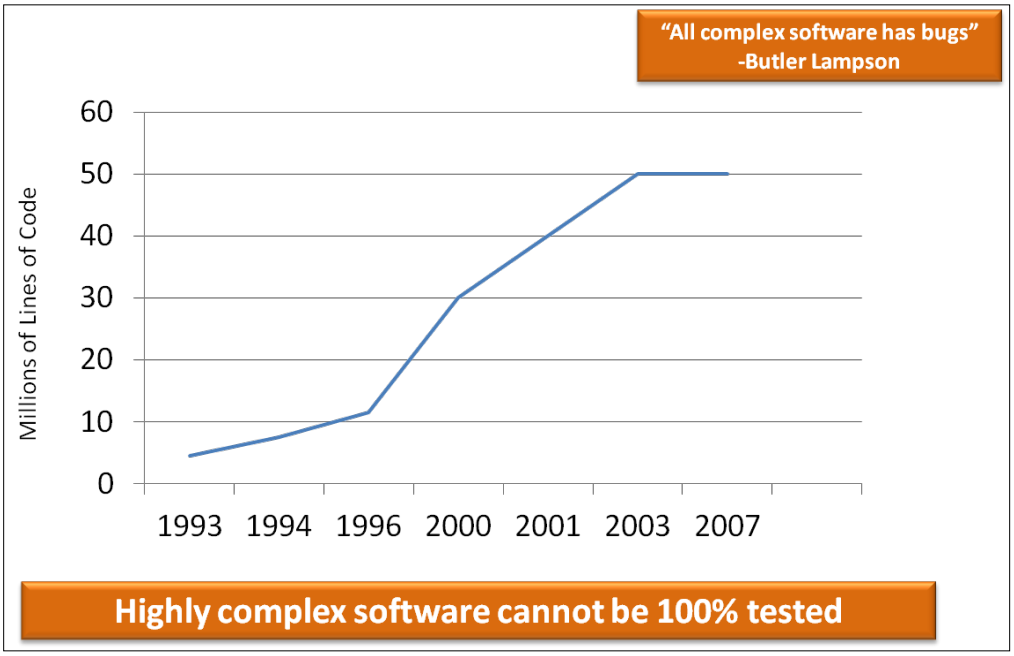

Figure 2.4 Commercial Operating System SLOC Growth

[14] Flight Software Complexity (https://acc.dau.mil/adl/en-US/.../FlightSoftwareComplexityBriefing_v5.ppt)
[15] DSB Task Force on Defense Software, November 2000; (Figure 3.4a)
[16] Pan, Jiantao; "Software Testing;" Carnegie Mellon University; Spring, 1999

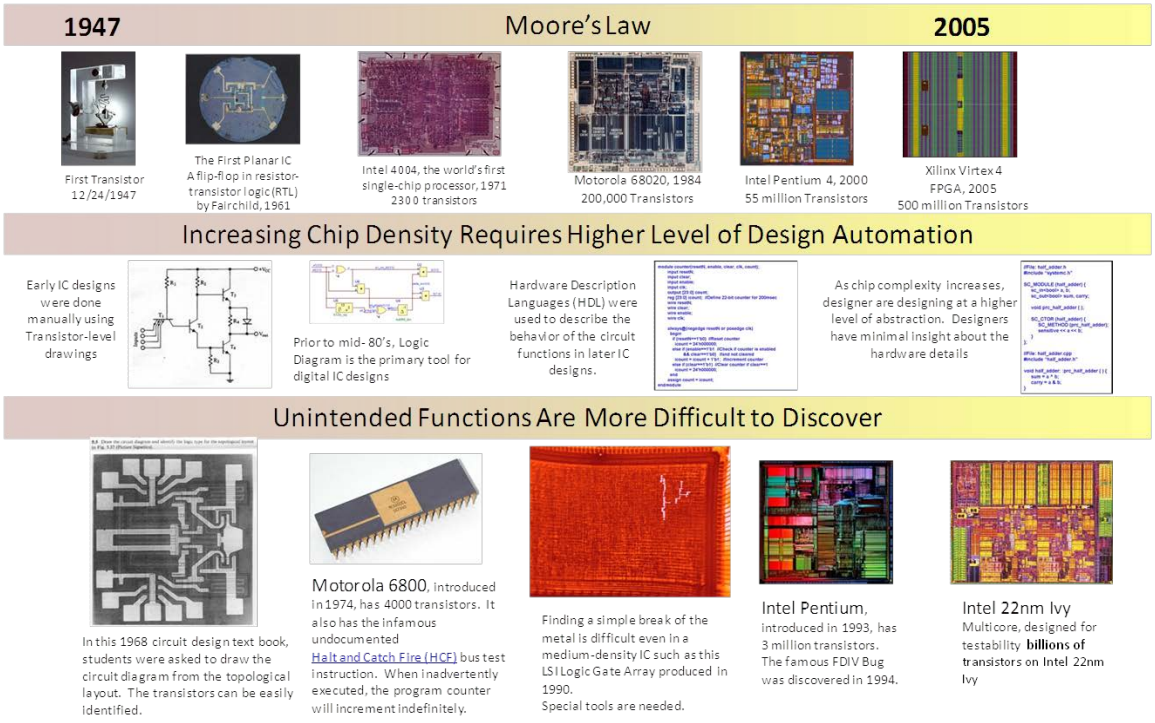

Figure 2.5 Representative Growth in Hardware Complexity

The realization and exploitation of vulnerabilities is clearly and abundantly illustrated in reports by the government and private security firms, and in the public press.[17, 18, 19, 20] The loss of U.S. intellectual property through cyber exploits has been estimated to be in the hundreds of millions of dollars, if not billions.[21] The vulnerability of the supervisory control and data acquisition (SCADA) systems controlling public utilities has been demonstrated[22,23,24] raising wide-spread concern that the Internet connectivity of these systems could lead to significant disruption of utility services (especially electricity) by malicious parties. Criminal organizations routinely substitute altered devices (e.g. fake ATMs and card readers) to intercept transaction data.

[17] DoD Strategy for Operating in Cyber Space, July 2011

[18] Statement of General Keith Alexander, Commander USCYBERCOM, before the Senate Committee on Armed Services, March 27, 2012

[19] AFP; Sophisticated cyber thieves behind Epsilon attack, April 6, 2011

[20] Wall Street Journal; Hackers Broaden Their Attacks

[21] Dowdy, John; "The Cybersecurity Threat to US Growth and Prosperity;" McKinsey & Company; 2011

[22] Industrial Control Systems Alert: MOXA Device Manager Buffer Overflow; ICSA-10-301-01; October 28, 2010

[23] Industrial Control Systems Alert: SPECVIEW Directory Traversal; ICSA-12-214-01; August 1, 2012

[24] Industrial Control Systems Alert: Increasing Threat to Industrial Control Systems; ICSA-12-046-01; February 15, 2012

Of particular concern to this Task Force is the theft of data from the government and defense contractors.

Another manifestation of potential threat actions receiving high-level DoD attention is seen in U.S. military exercises.[25] DoD red teams invariably penetrate DoD networks using Tier I and II threats. Such penetrations could seriously impede the operation of U.S. forces by degrading network connectivity, corrupting data, and gaining intelligence. Cleary, if U.S. red teams achieve adverse effects using lower level techniques, a sophisticated adversary could achieve even greater effects.

2.3 Consequences of and Reaction to the Threat

The accomplishment of U.S. military missions is critically dependent on networks and information systems. The threats described in the previous section may impose severe consequences for U.S. forces engaged in combat:

- Degradation or severing of communication links critical to the operation of U.S. forces, thereby denying the receipt of command directions and sensor data
- Data manipulation or corruption may cause misdirected U.S. operations and lead to lack of trust of all information
- Weapons and weapon systems may fail to operate as intended, to include operating in ways harmful to U.S. forces
- Potential destruction of U.S. systems (e.g. crashing a plane, satellite, unmanned aerial vehicles, etc.).

At the national level, one could posit a large-scale attack on the U.S. critical infrastructure (e.g., power, water, or financial systems). An attack of sufficient size could impose gradual wide-scale loss of life and control of the country and produce existential consequences. For such an attack to occur there must be an adversary with both the capability and intent to conduct the attack. A prudent course of action demands that the United States prepare for the possibility of such an attack given the uncertainties about how the future will evolve.

Given the severe consequences of the threat, the issue now is how to mitigate it, which is the subject of much of the remainder of this report.

[25] Director of Test and Evaluation 2011 Annual Report

3.0 Defining a Resilience Strategy for DoD Systems

To address the broad level of threats with a unified strategy, it was necessary to think through the threat, vulnerabilities, and consequences associated with these potential attacks. Figure 3.1 describes how the Task Force thought through this challenge. Risk is a function of the threat, the vulnerabilities of the systems to be protected, and consequences of compromise of the systems. The threat broke into two categories: intent of the adversary and their capabilities. Vulnerabilities are described as either inherent or operationally introduced and consequences, either fixable or fatal to the impacted systems.

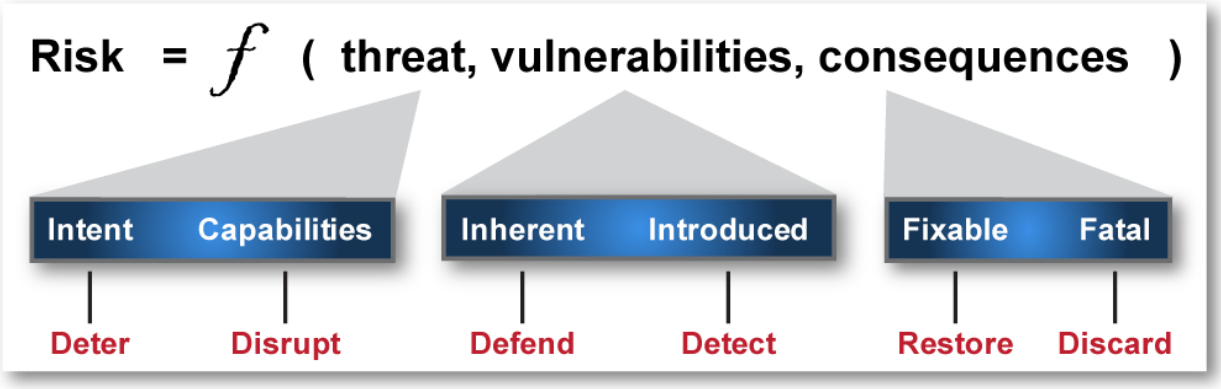

Figure 3.1 Risk Management Parameters

It is important to understand that the Task Force could not discover a credible mechanism to reduce the value of any of the three parameters (Figure 3.1), alone or in conjunction with the other parameters, to zero. Therefore, the threat, vulnerability and consequence parameters cannot be managed in isolation. A systems solution is required. Today much of DoD's money and effort are spent trying to defend against just the inherent vulnerabilities which exist in all complex systems. Defense only is a failed strategy.

DARPA produced Figure 3.2 that shows the growing gap between defensive and offensive software size. The complexity of the software defending our networks continues to increase exponentially over time due to increased complexity of the systems they attempt to protect, yet the size of software code used for the average successful attack remains nearly constant. This challenge is as old as the ages: the defense must protect against all possible offenses and the offense can mass all its resources against the weakest point of the defense. To address cyber risk, DoD needs a balanced approach across all three major parameters.

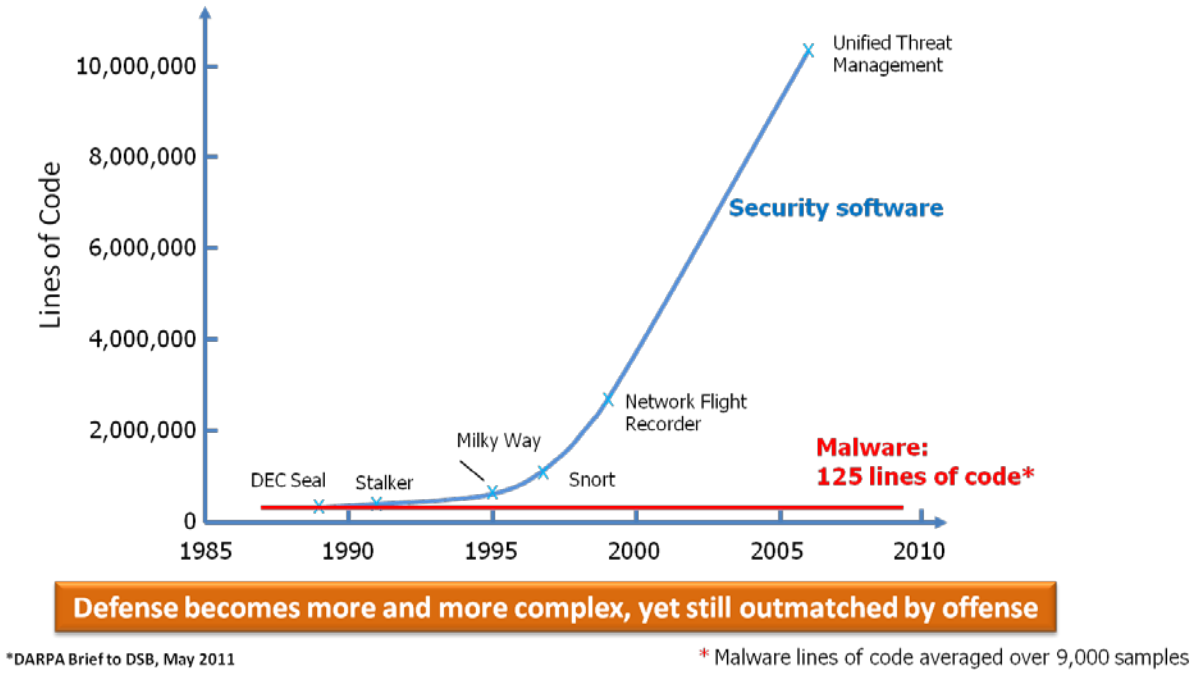

Figure 3.2 Graphic Illustration of the Complexity of Software Required to Defend and Attack our Systems. Very Small Changes (Even Single Bits) Can Cause Major Impacts to the Operation of a System

There is no single silver bullet to solve the threat posed by cyber-attack or warfare. Solving this problem is analogous to previous complex national security and military strategy developments including counter U-boat strategy in WWII, nuclear deterrence in the Cold War, commercial air travel safety and countering IEDs in the Global War on Terrorism. The risks involved with these challenges were never driven to zero, but through broad systems engineering of a spectrum of techniques, the challenges were successfully contained and managed.

There are several characteristics of the cyber challenge that collectively thwart our attempts to discover a closed-form solution to this national security issue. First, DoD's comprehensive dependence on this vulnerable technology is a magnet to U.S. opponents. DoD's dependency is not going to be reduced and will continue to grow. Thus, the adversary is not going away and their attraction to this weakness will increase. This adversarial persistence yields a **never-ending challenge**.

Secondly, there are no technical approaches that will comprehensively protect DoD against a determined adversary. DoD's diligent work over decades attempting to drive inherent vulnerability out of these systems and components has resulted in some progress, although DoD has barely begun to address the daunting problem of operationally introduced vulnerabilities into systems which is compounded by the large dependence on the global supply chain. In the face of the evolving cyber threat, DoD must recognize the limits to vulnerability reduction and the effectiveness of protection mechanisms and move to employ the threshold of "**good enough**" and work to reduce overall risk by managing all three risk parameters from a **systems perspective**.

Third, while there are many tests to demonstrate the vulnerability or weakness in a system, there will **never be a test** that demonstrates or proves the security of a system. This fact reinforces the need to seek "good enough" and the enduring existence of residual uncertainty.

Finally, because the opponent's advantage in exploiting/compromising/attacking DoD's information technology is substantial (game-changing), they will be highly motivated in their pursuit, innovative in their approach, and adaptive to U.S. strategy. The **adversary gets a vote** and this brings us back to the never-ending challenge. (However, they have many of the same risks to their systems).

The combination of these factors forces the United States to manage risk in this domain through a balanced systems approach.

This Task Force finds that without an urgently implemented and comprehensive strategy to offset the cyber security threat, U.S. national objectives will be nearly impossible to achieve in times of crisis. Additionally, the long term loss of so much intellectual property and capability will result in ***a serious competitive disadvantage*** to the U.S. economy.

Key findings of the study include:

- The cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War
- The cyber threat is also insidious allowing adversaries to access vast new channels of intelligence about critical U.S. enablers (operational and technical; military and industrial) that can threaten our national and economic security
- Current DoD actions, though numerous, are fragmented. Thus, DoD is not prepared to defend against this threat
- DoD red teams, using cyber attack tools, which can be downloaded from the Internet, are very successful at defeating our systems
- U.S. networks are built on inherently insecure architectures with increasing use of foreign-built components
- U.S. intelligence against peer threats targeting DoD systems is inadequate
- With present capabilities and technology, it is not possible to defend with confidence against the most sophisticated cyber attacks
- It will take years for the Department to build an effective response to the cyber threat to include elements of deterrence, mission assurance and offensive cyber capabilities.

The Task Force developed a set of recommendations that, when taken in whole, create a strategy for DoD to address this broad and pervasive threat to improve the resilience of DoD systems. Cyber is a complicated domain and must be managed across threat vectors to successfully address the challenges it presents. The cyber risk elements cannot be reduced to zero. While the problem cannot be eliminated, resilience capabilities can and must be

determinedly managed by the Department. Cyber risk can be managed through the combination of deterrence (up to a nuclear response in the most extreme case) and improved cyber defense. This strategy removes the requirement to protect all of military systems from the most advanced cyber threats, which the Task Force believes is neither feasible nor affordable. It will take time to build the capabilities necessary to prepare and protect our country from the cyber threat. **We must start now!**

3.1 Cyber Strategy for DoD

The following is the Task Force's recommended strategic approach to improving the resilience of DoD systems. The Task Force believes that these actions are in support of the published DoD Cyber Strategy.[26]

- Deter the Tier V-VI threat (raise confidence level that selected systems are protected from cyber attack and therefore available for deterrence)
  - Protect Nuclear Deterrent
  - Protect C2 and Continuity Of Government (separation of networks, war reserves)
  - Ensure some conventional strike and cyber attack capabilities to support escalation ladder (for theater operations as well)
- Minimize the impacts of Tier I-IV threats
  - Incrementally raise defenses
    - Instrument networks for intrusion detection and to provide situational awareness
    - Improve DoD cyber culture and personal responsibilities
    - Enforce universal practice of good hygiene
  - Evolve cyber requirements into DoD acquisition and support systems
- Improve critical capabilities important for both
  - Refocus intelligence collection to understand adversary cyber plans and intentions, and to enable counter strategies
  - Build a world-class cyber offensive capability with well-defined authorities and rules
  - Continue ongoing DoD efforts to develop secure system design and development capabilities, and to improve the security of the cyber supply chain

[26] See classified (SECRET) version of the May 2011 document titled: Department of Defense Strategy for Operating in Cyberspace

3.2 Table of Recommendations

Table 3.1 Table of Recommendations.

Description of Recommendations
1. Protect the Nuclear Strike as a Deterrent (for existing nuclear armed states and existential cyber attack).
2. Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary.
3. Refocus Intelligence Collection and Analysis to Understand Adversarial Cyber Capabilities, Plans and Intentions, and to Enable Counterstrategies.
4. Build and Maintain World-Class Cyber Offensive Capabilities (with appropriate authorities).
5. Enhance Defenses to Protect Against Low and Mid-Tier Threats.
6. Change DoD's Culture Regarding Cyber and Cyber Security.
7. Build a Cyber Resilient Force.

The Task Force anticipates that the implementation of the recommendations in Table 3.1 will be an ongoing effort, and establishing measures is an important step toward executing them. Without such tools, it will be difficult to tell whether or not progress is being made.

4.0 Measuring Progress

The Task Force attempted to define metrics that the Department could use to ultimately manage and shape cyber investments. Measures (used interchangeably with metrics for the contents of this report) are a critical part of any organization or business operation. They form a set of tools by which management determines and communicates the organization's highest priorities to the organization's employees. When done well, metrics act as an alignment tool in driving lower levels of an organization to make decisions consistent with strategies of their leaders. Moreover, the metrics become a mechanism to provide benchmarking, drive continuous improvement, and ensure sharing of best practices throughout an organization. Developing a set of cyber measures, which can be used across the Department to allow quantitative comparisons between options when making cyber (IT) investments and drive operational practices, is critical to increasing cyber resilience.

The Task Force set out to ascertain if useful metrics were currently available to determine or predict the cyber security or resilience of a given system. After several months of researching best practices of cyber metrics in commercial, academia and government spaces, the Task Force determined that no metrics are currently available to directly determine or predict the cyber security or resilience of a given system. Measures to predict cyber system resilience are difficult to create, due to the potential for small changes to cause discontinuous effects. A few critical bits manipulated in a weapon fire control system can render that weapon ineffectual. Millions of bits changed in a less critical portion of software may have only limited effect on the system. Even knowing if a system is compromised is very difficult. Often, when successful network exploits are identified, forensic analysis later shows the exploit lay undiscovered in the system for a year or more.

While difficult to measure cyber resiliency directly, the Task Force did find measures that could be implemented to improve the Department's defense posture and therefore indirectly improve its cyber resilience. To implement these measures however, the Department will have to develop common language and definitions, collection methods, and tools for collating data across the enterprise, and then use those results to drive decisions concerning future operations and personnel performance. This information will form the foundation for an education program that must be spread across the entire enterprise, to establish a common understanding. As experience is gained with these measures, and as more people understand the objectives and techniques, the metrics will evolve to become even more useful for the Department, providing a basis for measuring the effectiveness of future investments.

In a perfect world, DoD operational systems would be able to tell a commander when and if they were compromised, whether the system is still usable in full or degraded mode, identify alternatives to aid the commander in completing the mission, and finally, provide the ability to restore the system to a known, trusted state. Today's technology does not allow that level of fidelity and understanding of systems. When properly constructed, measures can guide design implementations and day-to-day operations to potentially fulfill these system goals at some

point in the future. Ultimately, a useful set of measures will help DoD leadership understand if they have prepared the Department to engage competitively in a conflict where cyber is a major component.

Measures must be chosen carefully. They must be leadership-owned and driven from the top. The most successful organizations implement a few carefully chosen metrics that balance between desired outcome, quality and delivery speed. There is an old saying that "you will get what you measure". As management puts its full force behind a strategy supported by a set of measures, their personnel will do what it takes to succeed at those measures, sometimes regardless of the end goal. Therefore, DoD management cannot treat cyber resilience measures as a fire and forget weapon.

The cultural aspects of metrics can be frightening to an organization embarking on this new path. Poor performance that may have been masked in the past could now be exposed. Management's tone on how performance issues are handled will determine whether organizations within the Department provide the minimum data required and attempt to hide from the spotlight, or see the measures as an opportunity to learn from others and improve performance at a faster rate. Ultimately, consistent and continuous improvement is much more important in the long run than the performance levels established at first baseline – good or bad. This Task Force defined an initial useful set of measures, based on collectable data that the Department could use to start down this path. It should be understood that to be successful, DoD leadership must take ownership and evolve this list into one of their own, to align the Department around a common strategy and set of agreed-upon measures. As experience is gained, the metrics will evolve. Building a culture of measurement used to drive continuous improvement and influence future designs and operations is a critical part of the process. Building a culture supporting measurement may seem like a trivial action, but from an historical and cultural perspective, this would be very new to the DoD.

Commercial organizations regularly use metrics to drive their strategies through their businesses, but it is nevertheless difficult to get initial metrics in place and operating. Establishing metrics should be an iterative process. Over time, and with consistent attention, the alignment of the organization to productive metrics provides great value and consistency in operations. The Task Force has developed two proposed metric panels; the first identifies the establishment of metric collection systems to implement Task Force recommendations, and the second defines performance measures that can be used once the systems are in place to give the Department an understanding of its cyber readiness. The goal is to offer the Secretary and his/her staff a couple of relatively simple charts that can be publicized and reviewed on a regular basis to track progress.

4.1 Metric Collection Systems

The Task Force created a notional metric collection system dashboard to monitor progress of strategy implementation. Before performance measures can be effectively implemented across the Department, collection systems must be put in place. The creation of a metric collection system provides a common language, definitions and standards to allow different organizations

in the enterprise to effectively communicate. In addition, the collection system develops reporting, tracking, analysis and display mechanisms for the collected data, to be useful to both Department leadership and managers closer to the front lines. This dashboard is a simple stoplight-chart measuring whether the building blocks required to implement the recommendations in this report are in place, useful, and effective. Note that Figure 4.1 does not represent a detailed DSB assessment of the current DoD status, but provides an illustration of how this tool can be used to drive improvement. The concept is to input data collected from relevant portions of the DoD and aggregate into a single block for each action. The ability to "click" on a block and view the background data on which it was based would allow front line supervisors to understand their performance relative to their peers and allow senior leaders to delve into problem areas and ensure adequate resources and attention are provided to improve performance.

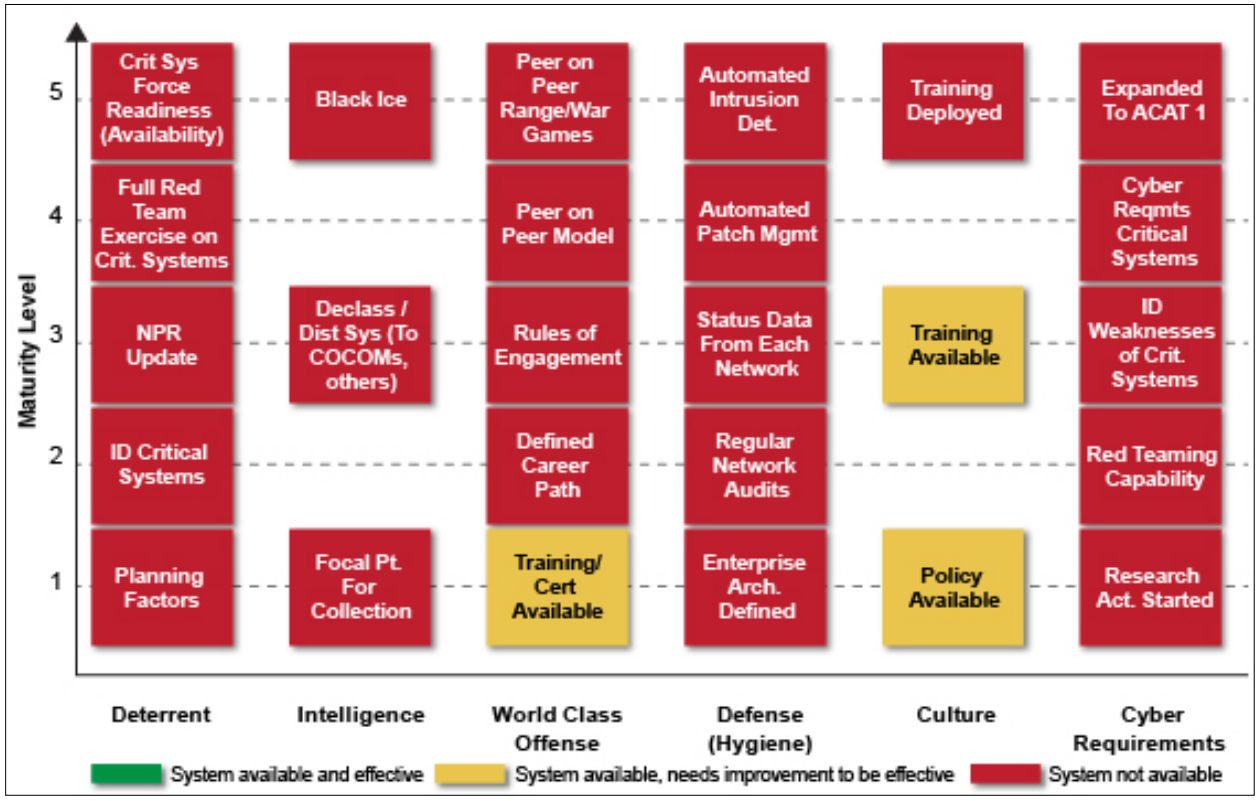

Figure 4.1 Notional Cyber Dashboard for Secretary – Metric Collection Systems

The blocks build on each major recommendation area from bottom (the simplest actions) to the top (most complex actions), leading to a maturity-level of accomplishment measure in building the required systems. As the systems come online, the next section outlines performance metrics that can be collected to drive system performance.

The metric collection system for each major recommendation area is crucial. For example, under the general area of defense/cyber hygiene, the metric collection system starts with developing a defined Department Enterprise Architecture. Creating a defined Enterprise

Architecture must drive common definitions of security posture and terms. In addition, the metric collection system devoted to Enterprise Architecture must identify reporting and tracking mechanisms that provide leadership the ability to monitor progress toward the intended goal. These mechanisms need not be complicated (e.g. a simple spread sheet will suffice). The next task requires developing a collection system to measure Regular Network Audits. The collection system must create common language as to what an audit is, how the Enterprise Standard will be audited, and the supporting reporting system (e.g. how often will audits be conducted and on what parts of the network etc). The objective of the audit collection system is to enable the Department to determine whether or not audits are conducted against defined standards. Auditing to standard language and terminologies will allow the Department to make comparisons between networks as data is collected. The next collection system builds off the lower blocks. Once a common enterprise is developed and audits can be conducted, a collection system to measure status of each network must be created. The collection system needs common terminology encompassing definitions of network and status followed by a reporting mechanism. This provides the foundation for an automated patch management collection system and finally, a metric collection system devoted to Automated Intrusion Detection—to identify how long it takes to find and remove successful intrusions into the network.

Other recommendation areas build similar metric collection systems. A deterrent collection system focuses on defining planning factors that include a cyber component for both strategic nuclear delivery platforms and NC3 (e.g. extension of the current USSTRATCOM planning factors to reflect cyber) and also applied to identification and segmentation of protected conventional capability for assured operation in a contested cyber environment. An intelligence collection system defines and builds out a focal collection point to enable sharing of information between the many communities affected by cyber. A cyber offense collection system should first define training and certification requirements which then will be used to build out a career path capable of providing the United States with offensive dominance. Developing a culture collection system starts with a cyber security policy articulated throughout DoD with clearly defined responsibilities and accountability standards. Finally, the cyber requirements collection system should focus on developing research and also on the development of a standard to address desired cyber resiliency features (e.g. the ability to maintain or return to a known trusted state, network and component awareness, etc) and then to track the incorporation of the standard into requirements and acquisition programs (acquisition category (ACAT) 1 programs first).

4.2 System Performance Metrics

Once collection systems are in place to execute the cyber strategy, the Department can begin collecting performance metrics. To jump to the end (outcome) metrics without the common enterprise standards, audit definitions, and an understanding of what the metrics mean, would generate little value. As an example, immediately gathering the number of cyber violations might appear to provide an indication of personnel compliance. However, if a cyber violation in organization A is not defined the same as a cyber violation in organization B then little is gained from such activity. Ultimately, the Department desires to measure outcomes, such as the

average time it takes to detect a successful attack that breaches the network perimeter defenses, and the amount of time it takes to recover a system that is lost as a result of a cyber attack.

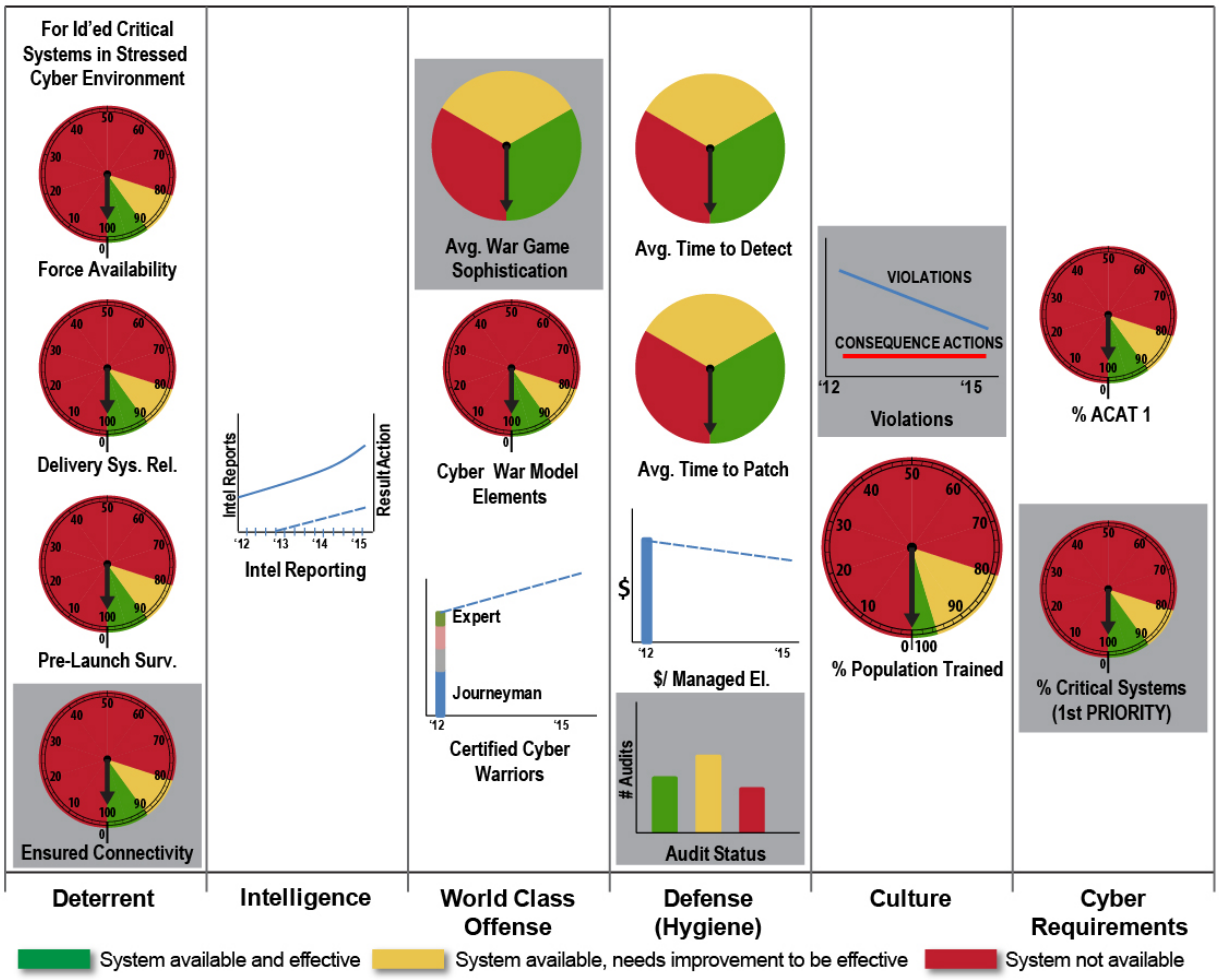

Figure 4.2 Notional Dashboard of System Performance Metrics

The Task Force estimates that within two years of gathering data, the DoD would have an experience base with the proposed metrics that would begin to allow comparisons of architectures, networks, and system elements for their contribution to cyber resilience and cost to operate. That data would provide DoD insight to inform predictions of performance of various architectures and elements versus available budgets.

The initial set of performance metrics should be kept small until sufficient enterprise experience is established to exercise quantitative assessment of progress. Once an initial set of performance metrics start to identify progress, additional performance metrics may be created. For example, an initial set of performance metrics addressing cyber culture simply measure the number of violations and personnel actions. Once the collection system is capable of accurately capturing this information, follow on performance metrics could be built to measure training responsiveness to new or specific attack vectors or measure training effectiveness by

conducting unannounced testing. Training costs could then be assessed by number of violations to both training events and real events.

Performance metrics in other areas should also yield useful information. The following suggested performance metrics identify specific knowledge the Department would use to address its cyber resiliency status. An initial defense hygiene performance metric focusing on the number of audits conducted to a known standard should support comparison of network architectures and operating costs. This is in stark contrast to the current state of auditing which, if done at all, is conducted across an assortment of standards and networks, resulting in the inability to derive enterprise knowledge. Performance measures to track offensive cyber can start simply with focus on the number of certified individuals against time. As baseline data becomes available, the Department will better understand its cyber posture and capabilities and can add more sophisticated measures to accelerate insight and drive progress.

5.0 Maintaining Deterrence in the Cyber Era

In the process of conducting this study, it became apparent that the full spectrum cyber threat represented by a Tier V-VI capability is of such magnitude and sophistication that it could not be defended against. As such, a defense-only strategy against this threat is insufficient to protect U.S. national interests and is impossible to execute. **Therefore, a successful DoD cyber strategy must include a deterrence component.** One key element of deterrence is the believable military capability to either defeat an attack or to provide a survivable response that holds at risk something the adversary highly values (i.e. the adversary's cost exceeds the adversary's gains). The top of that escalation ladder is the present U.S. nuclear deterrent.

The cyber threat highlights another key element of deterrence theory--attribution. Providing attribution against an isolated cyber attack can be slow and difficult. However the Task Force believes that attribution can be accomplished for attacks that would reach the level of really harming the country, because attacks of that scale require planning and multiple attack vectors--which usually leave clues. The Task Force believes attribution can be achieved for a sustained attack over a lengthy time period--whose integrative effects become catastrophic, as well as for a massive large-scale attack. In the former case, U.S. intelligence gathering is proficient at attribution when presented with sufficient time. In the latter case, large-scale attacks leave clues that provide attribution and even warning.

The ultimate goal is to protect the country and provide global stability. A deterrence strategy that encompasses cyber requires that the United States be viewed as a credible cyber force by those who may wish to present a challenge. The strategy will require an escalation framework with associated signaling and red thin-line strategies, and credible survivable military capabilities. The specific force-level and mix of military capabilities for this deterrence strategy requires further study that is beyond the scope of this report. However the Task Force believes a comprehensive deterrence strategy that addresses the cyber threat would certainly include offensive cyber and selected conventional military capabilities that are survivable and support a deliberate escalation ladder.

5.1 Background

The Nuclear Posture Review (NPR), published in April, 2010, provided the Obama Administration's roadmap for nuclear policy. It placed nuclear terrorism and proliferation as top priorities, along with reducing the role and numbers of nuclear weapons. One of the key conclusions from the 2010 NPR is given as follows:[27]

"The United States will continue to strengthen conventional capabilities and reduce the role of nuclear weapons in deterring non-nuclear attacks, with the objective ***of making deterrence of***

[27] Nuclear Posture Review Report, 2010

nuclear attack on the United States …the sole purpose of U.S. nuclear weapons" (emphasis added).

The United States would only consider the use of nuclear weapons in "extreme circumstances." The United States would not use or threaten to use nuclear weapons against non-nuclear states who are parties to the nuclear proliferation treaty.

The 2010 NPR did not refer to the "New Triad" (nuclear and conventional global strike, defensive systems, and responsive infrastructure) of the 2002 NPR, and instead called for continuation of the traditional Nuclear Triad (e.g. bombers, ICBMs, SLBMs), albeit with reduced warheads and delivery vehicles per the START Follow-On treaty between the United States and Russia. It is important in the context of this report that the 2010 NPR was essentially silent on relationship between the U.S. nuclear deterrent, indeed the U.S. strategic deterrence posture, and the domain of cyber and cyber warfare. Presumably one would characterize a catastrophic Tier V-VI adversary cyber attack on the United States as "extreme circumstances" in the public language of the 2010 NPR, so that is not precluded in the stated policy, but it is not explicitly mentioned.

Over the past decade, policy advocacy grew for a conventional global strike capability (2002 NPR, 2006 QDR). In these cases, there were essentially two arguments justifying a conventional strike capability:

1. To reduce the overall number and reliance on nuclear weapons by now holding nuclear targets at risk with precision conventional (non-nuclear) strike capabilities[28,29]
2. To offer non-nuclear global strike alternatives to national leadership in time-critical scenarios[30]

The Task Force concluded that the severity of the Type V-VI cyber threat resulted in adding a third reason for a non-nuclear conventional and cyber survivable strike capability with a special emphasis on "survivability":

3. To provide a non-nuclear but cyber survivable escalation ladder between conventional conflict and the nuclear threshold – that is to increase stability and build a new sub-nuclear red line in this emerging era of a cyber peer competitor delivering a catastrophic attack.

Despite the past decade of policy deliberations on new conventional global strike capabilities as part of a deterrence strategy, the situation today is such that the ultimate U.S. deterrent,

[28] 2002 Nuclear Posture Review Report
[29] 2006 Quadrennial Defense Review Report
[30] DSB Task Force on Time Critical Conventional Strike from Strategic Standoff, March 2009

including response against a catastrophic full spectrum cyber attack, is the nuclear triad–intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs), and nuclear-capable heavy bombers. The nuclear command and control (NC2) of the nuclear forces is comprised of systems, communication paths, and procedures associated with National Security Presidential Directive (NSPD)-28, which provides guidance to the Military Departments on the nature of redundant survivable communication paths to each nuclear delivery platform. Importantly, the definition of "survivability" in the traditional context of Nuclear C2 and forces usually referred to their credible ability to withstand a massive nuclear strike, with all of its attendant effects (including Electromagnetic Pulse (EMP)), and then provide a counter value retaliatory response. The Task Force expands the definition of survivability to include credible capability to withstand a Type V-VI cyber attack.

5.2 Recommendation: Protect the Nuclear Strike as a Deterrent (for existing nuclear armed states and existential cyber attack).

- SECDEF assign USSTRATCOM the task to ensure the availability of Nuclear C3 and the Triad delivery platforms in the face of a full-spectrum Tier V-VI attack – including cyber (supply chain, insiders, communications, etc.)

This Task Force recommends immediate action to assess and assure national leadership that the current U.S. nuclear deterrent is also survivable against the full-spectrum cyber Tier V-VI threat described in the taxonomy of this report. Note that a survivable nuclear triad within a full-spectrum, cyber-stressed environment is required regardless of whether or not one believes U.S. *retaliatory response with our nuclear forces* is a credible response *to a major cyber attack.* In other words, the basic characteristics of the traditional U.S. nuclear deterrent incorporates survivability as a basic precept; now the U.S. must add survivability in the event of a catastrophic cyber attack on the country as a basic precept.

5.3 Recommendation: Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary.

- SECDEF and Chairman, Joint Chiefs of Staff (12 months)

The Task Force is confident in the need for assured operation to all three – cyber, protected-conventional, and nuclear – capabilities, including their required C3I infrastructures, against advanced cyber threats. Further analysis is necessary to determine the optimal mix of these capabilities, especially the role of offensive cyber and protected-conventional to form the rungs of an escalation ladder designed to introduce elements of deterrence against Tier V-VI attackers. Recommendation 5.2 addresses the assured availability of the nuclear capability. Similar to the prior argument regarding the cyber resiliency of the nuclear deterrent, DoD must ensure some portion of its conventional capability is able to provide assured operations for theater and regional operations within a full-spectrum, cyber-stressed environment.

The Task Force addresses full spectrum cyber portion later (Chapters 7 and 8). However, the use of offensive cyber as part of an escalation ladder needs further study to determine where and how it can be effectively used. In particular, cyber's inherent stealth nature makes signaling difficult and deliberate signaling may divulge capabilities that then could be easily countered.

The Task Force identified the fundamental attributes of a survivable conventional strike capability comprising the protected-conventional rungs of the escalation ladder:

- Credible counter value effects on target(s) – globally and promptly
- Unambiguous signaling, as part of an escalation ladder, non-nuclear options, capabilities and intentions
- Reliable, safe, and secure; (High confidence of operation in a cyber contested environment)
- Treaty compliant
- Affordable – maximize use of existing systems and infrastructure
- Redundant and cyber survivable command and control (C2)

Because the expected cost of implementing cyber resiliency against V-VI threats is significant, the protected-conventional capability must support a very limited number of cyber- critical, survivable missions. Overextending cyber resiliency for all conventional capability will overwhelm DoD resources (technical, managerial, and financial). DoD must discipline itself to identify sufficient protected-conventional capability for assured operations. Furthermore, cyber resiliency can only be achieved by segmenting and isolating forces from general purpose forces. In the absence of a cyber threat, segmented forces are likely to possess slightly less capability than their non-segmented counterparts due to the isolation from every part of the supporting infrastructure which generates so much advantage to DoD. However, in the face of an adversary employing cyber, the segmented forces will provide far more capability than their non-segmented counterparts.

5.3.1 Segment Sufficient Forces to Assure Mission Execution in a Cyber Environment

Segmentation must differentiate only sufficient forces required to assure mission execution; it is not required across an entire capability. For example, if long range strike is a component of the protected-conventional capability, the DoD should segment a quantity sufficient to provide mission assurance in a hostile cyber environment (notionally, 20 aircraft designated by tail number, out of a fleet of hundreds, segregated and treated as part of the cyber critical survivable mission force). Segmented forces must remain separate and isolated from the general purpose forces with no dual purpose missions (e.g. the current B-52 conventional/nuclear mission).

As a starting point, the Task Force proposes the basic force elements comprising a protected-conventional capability take the form of a survivable second strike conventional mission described in Table 5.1 and listed below:

- Long Range Bombers with precision cruise missiles – currently operational with varying force mix options and numbers
- SSGN with long-range precision cruise missiles – currently operational with capability up through Tomahawk Block IV (offering an upper limit of greater than 600 weapons assuming four SSGNs at sea)
- Conventional ballistic missiles or ballistic/glide hybrids - none currently operational; experimental concepts being tested
- Survivable national and CCMD C2 leveraging nuclear thin line

The above supported by:

  - Build "true" Out-of-Band Command and Control for the most sensitive systems
  - War reserve simplified operating systems

5.3.1.1 SECDEF assign Unified Command Plan (UCP) Mission of Protected -Conventional Strike to USSTRATCOM.

- USSTRATCOM given target for initial operating capability (IOC) (24 months)
- USSTRATCOM provide desired planning factors (pre-"launch" survivability, Communications and C2 reliability, targeting/damage expectancy, etc) (6 months)
- USD(AT&L), in coordination with CIO, perform a system of systems (SoS) analysis on selected conventional strike capabilities to determine risk and define an acquisition plan to ensure an enduring survivable capability (6 months)
- Under Secretary of Defense for Policy (USD(P)) engage multi-agency counterparts for an updated Strategic Deterrence Strategy in 2014 NPR – cyber escalation scenarios on both sides (12 months)

  USSTRATCOM integrate offensive cyber capabilities, as described in Chapter 7, with protected-conventional UCP mission.

Table 5.1 Notional Elements of Protected-Conventional Strike Capability.

Precision Strike Platforms	C3
Submarines with Long Range (1000+ nmi) Cruise Missiles	Advanced EHF, ELF/VLF, Dedicated Fiber
Penetrating Bombers	CCMD & Senior Leader Decision Tools & Displays
Long- Range Conventional Missiles	Emergency Action Messages (EAMs) for Conventional Strike ("CAMs")

5.4 Conventional Deterrent Measures

Figure 5.1 shows measures proposed to support the creation of a conventional deterrent as an escalation path to our nuclear deterrent. The establishment of the system performance measures in the previous Chapter called for (starting at the bottom of figure 4.2) the establishment of planning factors, the selection of the "critical systems" that would be included as part of the conventional deterrent, and acquisition plans to bring those capabilities online. As the identified critical systems are modified and built, they would be measured for availability in a stressed cyber environment. Since this is expected to be a relatively small number of systems, each would be measured through analysis, testing or war games for:

- Connectivity to leadership C2 (President of the United States (POTUS)/USSTRATCOM)
- Prelaunch survivability of the system
- Reliability of delivering payload to target

It's envisioned that each measurement would be in the form of a calculated availability from test and analysis results. The "rolled up" average across systems would be displayed on a dial chart, with red, yellow and green portions as availability is increased. The calculated combination of these three measures provides a force availability measurement of our conventional deterrent capability in a stressed cyber environment. While it may take several years to build the maturity in the systems to be able to populate the force availability metric, the experience gained producing the connectivity, survivability and delivery metrics build to that ultimate Force Availability result.

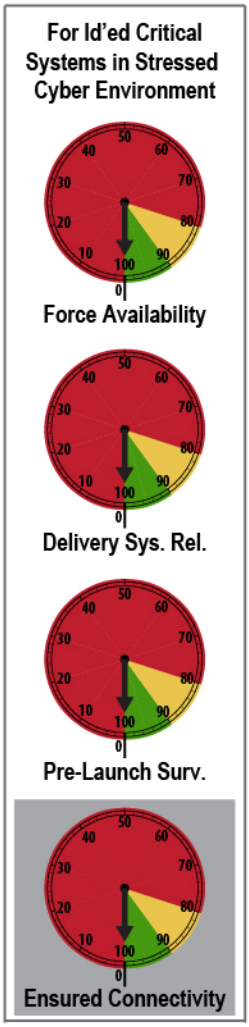

Figure 5.1 Conventional Deterrent Measures

6.0 Collecting Intelligence on Peer Adversaries' Cyber Capabilities

6.1 Background: Scope of Higher-Tier Threats

The Task Force received briefings on widespread intrusions and the theft of significant amounts of technical information from government and U.S. industrial base networks. There is ample open source evidence to indicate that adversaries are planning high-end attacks. Chinese doctrinal writings[31] on cyber and asymmetric warfare portend that country's use of cyber-based means to disconnect and disable U.S. Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) and DoD fighting elements in the event of a conflict. The widespread theft of intellectual property (IP) from the DoD and U.S. industrial base, could position prospective adversaries with the knowledge needed to employ countermeasures to advanced U.S. military systems, and also shorten a given adversary's research and development timelines for such countermeasures. The Task Force was briefed on Internet-based threats to information systems that originate abroad as well as within CONUS, using "hop points" to avoid some U.S. countermeasures that can only be used against foreign-based threats. These cyber-based capabilities provide a baseline from which to develop and field offensive cyber tools aimed at denying U.S. access to systems and networks.

While the cyber realm presents asymmetric vulnerabilities to networked systems today, high end threats have been around for a long time, and are not confined to software and network operations. During the Cold War, for example, the United States knew of widespread Soviet theft of US intellectual property, and implemented a program to counter the theft.[32]

The importance of countering cyber threats to U.S. National Security is increasingly recognized by U.S. leadership. In a recent hearing before the Senate Select Committee on Intelligence, FBI Director Mueller said "I do not think today it [cyber] is necessarily the number one threat, but it will be tomorrow. Counterterrorism and stopping terrorist attacks, for the FBI, is a present number one priority. But down the road, the cyber threat, which cuts across all programs, will be the number one threat to the country."[33]

6.2 Recommendation: Refocus Intelligence Collection and Analysis to Understand Adversarial Cyber Capabilities, Plans and Intentions, and to Enable Counterstrategies.

- SECDEF, in coordination with the Directors of the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and the Department of Homeland Security

[31] Oakley, John, "Cyber Warfare: China's Strategy to Dominate in Cyber Space," 2011; US Army Command and General Staff College

[32] Weiss, Gus W (1996), "The Farewell Dossier: Duping the Soviets", *Studies in Intelligence* (Central Intelligence Agency)

[33] Transcript, 31 January 2012 Senate Select Intelligence Committee open hearing on worldwide threat

(DHS), should require the DNI to enhance intelligence collection and analysis on high-end cyber threats. Request the creation of an Intelligence Community-wide implementation plan that defines implementable enhancements, and their resource impact on DoD, DHS elements CIA and FBI. (12 months)

Subversions of sophisticated hardware and software systems are extraordinarily difficult to detect through testing and inspection. This led the DSB Task Force to conclude that deeper intelligence about adversaries' offensive software and hardware tools is essential to counter high-end, state-sponsored cyber threats, because it can help focus U.S. efforts on likely targets of compromise.

This intelligence must include the following:

- Identification and understanding of adversarial cyber weapon development organizations, tools, partnerships (e.g., supply chain), leadership, and intentions;
- Development of targeting information to support initiatives to counter cyber weaponization;
- Accurate assessment of adversarial plans and capabilities for policy makers.

Previous DSB reports have addressed both the importance of intelligence and the associated challenges of meeting these intelligence requirements. Based upon the impossibility of sufficiently mitigating a Tier V-VI threat without filling these intelligence gaps and the national security impact of not effectively addressing this threat, the Intelligence Community must increase the priority of its intelligence collection and reporting requirements in this domain.

6.2.1 In response to state sponsored threats, the Task Force recommends the creation of a counterintelligence capability to directly address the most sophisticated threats using tools and techniques derived from both defensive and offensive U.S. cyber programs.

- Additional details are provided in Appendix 6.

6.3 Intelligence Performance Measures

It is essential that organizations throughout the Department (and the United States Government) understand what impact cyber attacks are having on government systems, and what is being done to counter such attacks.

Organizations in the Department today, however, do not generally share details about cyber attacks that have compromised their systems. Instead, system compromises are often classified, keeping people in the dark who must be aware so they can anticipate similar attacks. Consequently, DoD organizations are trying to field defenses based only on partial knowledge of what kind of vulnerabilities are being exploited.

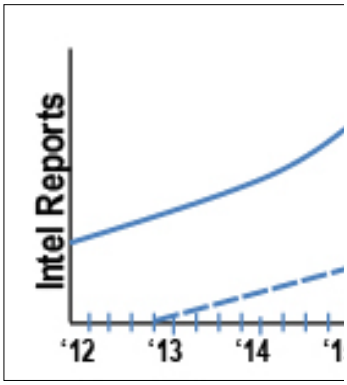

Figure 6.1 Intelligence

Early performance metrics in intelligence, as illustrated in Figure 6.1 would track the number of reports generated, and the number of those reports that actually generated changes to our systems to better protect them. Further refinement could include a feedback mechanism to track adversary reaction to the initial changes enabled by intelligence.

7.0 Developing World-Class Cyber Offensive Capabilities

7.1 Background

To prevent the threat of cyber attack from limiting U.S. freedom of action in the global economic and political system, no strategic competitor or adversary can be allowed to gain (or mistakenly believe that they have gained) offensive cyber superiority. The U.S. must be a superior competitor in the cyber domain. Current trends, however, could lead some of our country's adversaries to believe that their offensive cyber capabilities, together with their mission-critical defensive postures, are sufficient to neutralize current U.S. conventional or nuclear force capabilities, and thereby hold at risk critical U.S. infrastructures vital to the Nation's economic, political and military operations. Cyber offense is both an enabler for military operations and, as argued in previous chapters, is a critical rung in the escalation ladder for U.S. deterrence strategy.

Offensive cyber operations require *sustained privileged access* to a target system or network. Gaining such privileged access is challenging for most targets of military interest. One must discover or create useful vulnerabilities to gain access, and escalate privilege. Moreover, the existence of this avenue must remain undiscovered by the target for significant periods of time. Target system or network configurations are subject to unexpected changes and upgrades, so an avenue of access that worked one day might not work the next. The adversary can also be expected to employ highly-trained system and network administrators, and this operational staff will be equipped with continuously improving network defensive tools and techniques (the same tools we advocate to improve our defenses). Should an adversary discover an implant, it is usually relatively simple to remove or disable. ***For this reason, offensive cyber will always be a fragile capability.***

Cyber offensive weapons also add a new complexity to warfare. Unlike a conventional bomb, where once it detonates has no further military value, a cyber weapon, if not carefully designed, can be potentially reused by the enemy or "bounce back" and potentially threaten our own systems.

Discovering which of an adversary's system and network components are useful targets requires full-spectrum intelligence support. Intelligence support assets are almost always in short supply and, in the case of those needed to support offensive cyber planning, the shortage is even more acute. In some cases, a component of the system or network of interest may already have been fitted with some level of access arising from non-offensive cyber intelligence priorities. Such access may be helpful but still not offer the granularity needed for precise military targeting. For example, an intelligence agency may have access on a network used for

intelligence exploitation and USCYBERCOM[34] may desire to develop an order of battle plan against that target. Intelligence interest may stop at a server or router in the network, to conduct intelligence operations at those points. USCYBERCOM's mission requires situational awareness and access down to the terminal or device level in order to support attack plans. USCYBERCOM would need to work with intelligence agencies to ensure the portions of the system they disable don't disable critical intelligence assets. In other cases, no pre-existing access will be in place and the access effort must start from scratch. History shows that such situations can take a long time (i.e., months or years) to achieve results.

Given the potential stealth (e.g. widespread deployment of relatively undetectable "sleeper malware") and much more compressed time scales likely to be associated with cyber conflicts, a much better understanding of the dimensions and escalatory consequences of such conflicts is needed. Of special significance is the possibility that a well-orchestrated, pre-emptive cyber strike by an adversary, who is able to fully integrate multiple cyber and non-cyber capabilities, could render the U.S. incapable of using any of its own offensive capabilities for a retaliatory strike. The time-honored principles of Initiative and Offense will undoubtedly remain paramount in cyber conflict strategy and doctrine.

U.S. policy must clearly indicate that offensive cyber capabilities will be utilized (preemptively or in reaction; covertly or overtly), in combination with other instruments of national power, whenever the National Command Authority decides that it is appropriate. The recent DoD Cyber Strategy leaves this option open and discusses potential U.S. responses to cyber attack. The appropriate authorities must exist with those responsible to protect U.S. interests.

The intellectual and empirical underpinnings for strategy and doctrine for kinetic, nuclear, counterterrorism, counterinsurgency, and other missions have been extensively documented and debated for decades. Most modern militaries have adapted these underpinnings to their own situations and have implemented them within their own contexts. In contrast, relatively little has been documented or extensively debated concerning offensive cyber operations. This is especially true with respect to the use of offensive capability as a component of a larger strategic deterrence that, to be effective, must achieve visible results against the adversary but not reveal enough about the capability for an adversary to create a defense. DoD should expect cyber attacks to be part of all conflicts in the future, and DoD should not expect adversaries to play by U.S. versions of the rules (e.g. should expect that they will use surrogates for exploitation and offensive operations, share IP with local industries for economic gain, etc.)

[34] USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure US and allied freedom of action in cyberspace, while denying the same to our adversaries.

USCYBERCOM, and its supporting Service Component Commands, must be the driving force to surface the doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) /Unity-of-Effort gaps and advocate for requisite gap-closure actions. The Intelligence Community and other United States Government Departments and Agencies, with distinct and overlapping authorities, also have key supporting responsibilities. Given the nation's cyber defensive posture, time is of the essence in developing a broader offensive cyber capability.

7.2 Recommendation: Build and Maintain World-Class Cyber Offensive Capabilities (with Appropriate Authorities).

7.2.1 Commander USCYBERCOM Develop a Capability to Model, War Game, Red Team and Eventually Train for Full Scale Peer-on-Peer Cyber Warfare.

- Select an FFRDC-like Center of Excellence. (within 6 months)
- Develop capability to model peer-on-peer (red & blue with supporting situation awareness tools and techniques) full scale conflict, similar to nuclear exchange models (trigger uncertainties, deliver link probabilities, blow-back risk, recovery abilities and timelines, etc.) (IOC within 18 months of contract award)
- Develop model and validate—evolve through red team and cyber range/war game exercises. Move beyond tabletop level of sophistication. (IOC within 18 months of modeling capability)

Planning for and successfully executing a single offensive cyber operation requires a significant set of competencies (e.g. computer science, engineering, encryption, linguistics, geo-political context, military planning and targeting, and more). Given peer and near-peer adversaries who may wish to challenge the United States via cyber aggression, the DoD must develop the capacity to conduct many (potentially hundreds or more) simultaneous, synchronized offensive cyber operations, while defending against a like number of cyber attacks. Today, U.S. activities are focused on individual targets in relatively static environments. Understanding interactions and dependencies involved in large scale cyber battle will be required to plan the battle, determine the scale of forces required, and conduct operations at time of conflict.

This situation is similar to when the United States was at the end of WWII, with the newly developed nuclear bomb. It took decades to develop an understanding of how to best use the weapon, and the strategies to achieve stability with the Soviet Union (based on mutually assured destruction). Much of that work started at The RAND Corporation, an FFRDC, with toy rocket surrogates and table top exercises, growing over time into sophisticated simulations and tests that led to strategies for protecting the country. The United States should expect that a similar kind and level of effort will be necessary to mature its understanding and strategies for the use of cyber offensive capabilities. Unfortunately, the Task Force could find no evidence of modeling or experimentation being undertaken to better understand the large-scale cyber war. NSA's recent "red flag war game" is one of the few exceptions that have begun to explore the implications of large-scale cyber operations during the fog of war.

Modeling and understanding a peer-on-peer conflict, with many sorties taking place at once, triggering mechanisms for our own attacks coming and going as networks go offline, addressing blowback of attacks onto its own assets, etc., will be a very complicated undertaking. Even more challenging is that, unlike use of a nuclear weapon (presumably under only extraordinary conditions or threat), cyber attacks are expected in every future conflict, and as discussed earlier in the report, the most significant vulnerability is in the U.S. critical infrastructure on which both the military capabilities and civilian populations depend. To determine the scale of forces needed and the optimal strategies to defend our country, a robust understanding of large scale cyber offense is required. Moreover, the adversary gets a vote. Cyber war is unlikely to be fought as the United States might like to assume it will be. The United States must be ready to adapt to an adversary that is willing to create its own rules.

7.2.2 USD(P) should establish a policy framework for Offensive Cyber Actions to include who has what authority (for specific actions), under what circumstances, under what controls.

- Completion Date: 18 Months

The appropriate authorities must exist with those responsible to protect U.S. interests. Cyber actions can take place in very short time periods and those responsible to protect the country must understand their roles and authorities. This Task Force has not extensively studied or made recommendations about the definition of "appropriate authorities." Several other efforts are underway in the administration to address this issue and DoD is only one of many players in the broad protection of the United States against cyber attack.

7.2.3 Commander, USCYBERCOM to increase the number of qualified cyber warriors, and enlarge the cyber infrastructure commensurate with the size of the threat.

- Completion Date: 18 Months

The DoD has qualified cyber warriors on the job today, supported by robust training programs and cyber toolsets. However there appears to be a "burnout factor" beginning to exhibit itself among these elite people. The Department must scale up efforts to recruit, provide facilities and training, and use these critical people effectively. The Task Force believes there is general agreement today that more cyber warriors are needed, however, no conclusion on the ultimate size for which the department should plan has been reached. Executing this recommendation will generate a requirement for the cyber warrior force size.

7.2.4 USD(P&R), in collaboration with the Commander, USCYBERCOM and the Service Chiefs establish a formal career path for DoD civilian and military personnel engaged in "Offensive Cyber Actions"

- Address training and certification requirements

- Define career designations
- Define incentives for personnel achieving higher levels of certification
- Ensure that there is a cadre of high-end practitioners
- Completion: 18 Months with quarterly reviews with the DEPSECDEF

"Cyber Warrior" is a new domain for the Department, and this new class of job will require career paths, training expectations and incentives to attract and develop the needed expertise. It is not clear that high-end cyber practitioners can be found in sufficient numbers within typical recruitment pools. The DoD has the ability to define what it needs and adjust its personnel policies to enable achievement of that goal.

7.3 World-Class Offense Measures

Building a world-class cyber offense is already well on its way within the Department. The elements needed to ensure a successful capability are:

- A sufficient number of trained cyber warriors
- A formal career path to allow cyber expertise to be rewarded
- The ability to model and simulate peer-on-peer cyber conflict at scale
- The ability to conduct war games against Tier VI capable adversaries

Notional system performance metrics are depicted in Figure 7.1. The first proposed metric is the simple measure of the number of certified cyber warriors over time. The measure would also include a breakdown of the levels of capability comprised within the total number. By tracking the number over time, the Department can ensure it is growing the number of cyber warriors. As modeling and simulation capabilities are further developed, the DoD will be able to project the needed levels of cyber warriors to conduct potential expected operations. At that point a target would be added to the metric.

The second metric focuses on the ability to model and better understand peer-on-peer cyber warfare. The proposed metric is a dial scale building from today's limited understanding of single and small numbers of attacks based on a few network elements up through developing the ability to model and simulate conflicts with hundreds or even thousands of simultaneous events.

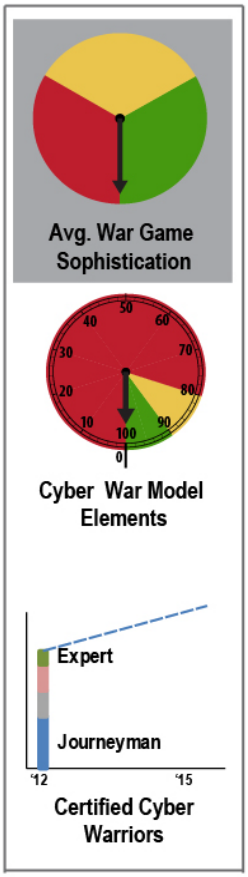

Figure 7.1 World-Class Offense Metrics

The final metric is a measure of war game sophistication. Today most war games and red teams are conducted using low and mid-Tier attack capabilities only. The NSA's recent Red Flag exercise was one of the first attempts at measuring systems against more advanced attack capabilities. DoD must build cyber ranges that can be isolated and controlled, yet still operated at a reasonable scale to continue to develop understanding of the vulnerabilities of operational

systems against attacks up to Tier VI sophistication. This measure would take an average of all red teams and war games conducted in any period by the level of sophistication of the threat used in each exercise.

8.0 Enhancing Defenses to Thwart Low- and Mid-Tier Threats

8.1 Background

For more than 15 years, the Department has invested significant resources (people and funding) in an effort to prevent, detect and respond to a full range of cyber threats. Recognizing the interdependency of DoD systems and networks, there has been an attempt to put in place a formal framework and integration capability (Defense-Wide Information Assurance Program and Global Information Grid Information Assurance Program) to provide coherency to the individual Service and Agency programs. The Information Assurance (IA) Component of the DoD Global Information Grid, approved in 2005 provided a broad architectural baseline for implementation of IA and network defense measures.[35] Strong authentication based on the Common Access Card (CAC) and Public Key Infrastructure (PKI) capabilities and other Defense in Depth mechanisms added to the overall "assurance" of the networks. Then, based on a significant infection of the Unclassified but Sensitive Internet Protocol (IP) Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet)in 2008, deployment of additional technologies, e.g., Host Based Security System (HBSS) and other hardening and situational awareness tools were accelerated.

While well-intentioned and strongly supported, these and subsequent initiatives have not had the desired impact on the overall IA posture of the Department. Defensive measures implemented at the boundaries between the NIPRNet and the Internet proved to be only marginally effective in blocking successful intrusions or reducing the overall attack surface of DoD networks and systems. Mobile platforms (smart phones, tablets, etc.) exacerbate this already challenging problem. Red teams, conducting operations during military exercises or at the request of Military Department and Agency officials, continue to have a nearly perfect success rate breaking into the systems.

Within classified networks, once thought to be safe for military command and control traffic, our adversary has successfully penetrated vulnerabilities created by poor user practices and a lack of discipline at all levels of the command structure. Operation BUCKSHOT YANKEE was clearly a wake-up call, suggesting that *every* system relied on for the conduct of war fighting operations is at risk of exploitation by an increasingly sophisticated adversary; an adversary ready and able to exploit any technical or human weakness to achieve their objectives. After-action reports, long after the detection and mitigation of this serious infection of a classified network, continue to point at residual weaknesses. Heightened awareness, enhanced detection capabilities, and greater accountability of everyone concerned with activities involving the network have not fully eliminated the threat vector originally leveraged in BUCKSHOT YANKEE.

[35] DoD 8570.01-M; Information Assurance Workforce Improvement Program, December 19, 2005

The complexity of systems and networks, connectivity and interdependence (with other DoD, contractor and commercial provider networks); inadequately trained (and overworked) system administrator and maintenance personnel; lack of comprehensive automation capabilities that would free trained personnel to focus on the most serious problems; lack of broad visibility into situational awareness of systems and networks and inadequate or non-existent Mission Assurance Strategies and Plans all contribute to a "Readiness" level that is well below what is appropriate or needed for the Department to project power in the face of the asymmetric threat facing the Nation today. These issues have been the subject of numerous studies, reports, briefings and discussions between all levels of the Department, yet forward progress remains slow while the threat continues to grow rapidly.

The DoD CIO's IT Modernization and Joint Information Enterprise initiative recognizes and addresses many of the existing shortcomings. This effort focused on:

- Collapsing networks
- Providing for a single authoritative source for Directory and Access
- Consolidation of Datacenters
- Common Enterprise Services
- Effective Enterprise governance to achieve compliance
- Adequate funding

The effort to date is not measurably different than previous attempts (implemented through the Defense Information Assurance Program (DIAP) and the Global Information Assurance Portfolio (GIAP) to achieve similar ends. This effort must be expanded to include a specific Enterprise Architecture (EA) that becomes *THE* target architecture for every Military Department and Agency within the DoD.

8.2 Recommendation: Enhance Defenses to Protect Against Low and Mid-Tier Threats.

8.2.1 Establish an enterprise security architecture, including appropriate "Building Codes and Standards", that ensure the availability of enabling enterprise missions. The architecture should allow for the ability to:

- Segment the network
- Provide continuous monitoring and situational awareness
- Automate patch and threat management functions
- Audit to the enterprise standard
- Recover to a known (trusted) state
- Provide out-of-band command and control for most sensitive systems

- Responsibility: DoD Chief Information Officer (in collaboration with Military Departments and Agencies). (6 months)

While the Department's size (about 6 million devices connected to the networks) makes this problem challenging, DoD is made up of individual network segments that are connected together, just like everyone else's networks. Examples of similar (but smaller) network structures from the larger contractors in the defense industrial base offer valuable lessons for the DoD.

In 2005, a number of DoD contractors were the victims of advanced cyber attacks. Then Deputy Defense Secretary, Gordon England, held a meeting with the CEOs of the Department's biggest suppliers and laid out a plan for what became the Defense Industrial Base (DIB) Cyber Security/Information Assurance (CSIA) Pilot program, which enabled these suppliers to share information on cyber attacks and work with the government to protect its networks. A side benefit from the DIB-CSIA pilot was the education of the CEOs about the risk and the importance of deploying a strong defense across their organizations.

The result of the focus on securing their corporate networks drove the development of network security teams, led by a Chief Information Security Officer (CISO), chartered to develop and publish network standards (typically based on National Institute on Standards and Technology (NIST) network standards) that are used by the operating divisions of the company. Networks are segmented and managed separately within the larger organization structure, but under the monitoring and influence of the CISO. Employees are trained and held accountable for their actions, networks are monitored around the clock and threat vectors are shared across network segments. Most importantly, each network segment is audited (including, penetration testing as well as compliance checks) on a regular basis, and segment organizations failing these audits must report to the CEO and Board of Directors on plans to correct the weaknesses. The Board of Director's Audit Committee tracks progress through completion. This commitment and follow-through by the CEOs have made cyber security a high priority within these companies.

While these companies are not able to block all mid and high tier attacks, and still are not perfect against lower-tier attacks, they have made it much harder (more expensive) for attackers to succeed, reduced the "noise level" on their systems, and freed resources to focus on hunting intruders within the network (anomaly investigations).

DoD represents a larger target and must also deal with operating military systems in addition to the IT structure, but the same concepts are useful. DoD has already put in place some of the pieces, but establishing an enterprise level architecture and achieving consistent compliance is still missing. Appendix 5 contains an example Enterprise Specification.

Finally, DoD has a history of providing network waivers too readily for new systems coming online. While waivers are occasionally necessary, they almost always weaken the network's security status. Waivers that deal with out-of-date legacy equipment should be eliminated by the creation of enclaves and installation of firewalls. And, generally, DoD needs to be considerably less liberal about issuing waivers. The discipline of avoiding waivers for new systems will have a strong impact on the ultimate security posture of DoD networks.

The goal of a consistently applied and managed architecture across the Department is to take the low-tier threats off the table, thereby reducing the noise level on DoD networks. More effective mitigation of mid and high tier threats then becomes feasible.

8.2.1.1 Segment the Network

The Department already operates a mesh of networks that can be controlled independently. That concept should be extended through all operational war fighting systems, and tests/trials/red teams should be conducted to understand the capabilities and impacts of disconnecting an infected network to prevent infection of other, interconnected networks.

8.2.1.2 Provide Continuous Monitoring and Situational Awareness

An additional challenge for DoD is understanding who is "on" and what is the operational status of their network(s). Sensor deployment has begun at Internet access points to monitor and control access and network traffic flow. These Einstein sensors provide monitoring of network ingress and egress through a system of mostly COTS network monitoring tools driven by the NSA-provided signature set. This is a good start, but commercial tools have advanced to include capabilities to operate behind firewalls and to track anomalous activity throughout the components of a network. It is essential to provide continuous monitoring of all networks against cyber attack (see State Department example in Figure 8.1).

The information assurance of operational systems is typically achieved through encryption of data during network transport (and occasionally at rest - while stored) or multi-level security solutions geared toward the safe handling of multiple security levels of data on the same computer (processor). Data must be decrypted prior to processing, and advanced attacks being used today access the data at that point, thereby circumventing the encryption.

Little consideration goes into military system design today on providing test points that can report system health and operation (sensors). Are checksums overflowing in the processor? Is the processor conducting unexpected computations? There are many "tells" (symptoms) that could be detected and reported. Although such test points and their data transmission would also become targets for cyber attack, an adversary must now have a more detailed understanding of system internals to design a successful attack. The adversary would also be required to break into two systems (the main mission and test/sensor system) and change both correctly without setting off alarms to successfully infiltrate the system – a much more difficult task.

In the recent wars, DoD once again learned the value of timely, detailed situational awareness on the battlefield and invested heavily in Intelligence, Surveillance and Reconnaissance (ISR) assets. The United States must now build the same level of understanding into its networks and weapon systems.

8.2.1.3 Automate Patch and Threat Management Functions

Much of network management in the DoD relies on manual tasks performed by overworked network technicians and administrators. The scale of manual efforts is largely driven by legacy systems using unsupported software operating systems and the lack of consistency in network technology implementation across the Department. The recommendation to isolate systems utilizing older software (no longer maintained by commercial industry) means those systems are removed from the group of components that is regularly updated for malware and other software attacks and then assuming that those systems are likely compromised. The larger GIG is then protected from those systems through strong interface firewalls and detection software. The remaining "compliant" systems can then utilize modern COTS network management software and automate much of the effort required to detect intrusions and push software patches across the network.

Over time, fewer staff should be needed to maintain software patches and network configurations, allowing a shift in effort toward hunting adversaries who have penetrated our networks. Most of the COTS technologies available today have user interfaces that allow high levels of flexibility for determining what is deemed unusual network behavior, allowing system administrators to adjust and adapt the monitoring systems as threats evolve.

8.2.1.4 Audit to the Enterprise Standard

Conduct audits and in-process reviews to develop migration and mitigation strategies (systems that cannot be maintained in a timely matter should be restructured into enclaves and isolated from the GIG through firewalls).

The most important part of the recommendation concerns accountability and consistency that must come from senior leadership support and enforcement. Without this management imperative, an attempt at cultural change to improve cyber security will not be taken seriously within the Department.

A useful example of management proactively supporting a cyber standard and driving organizational acceptance is found within the Department of State (DOS). Several years ago the DOS CIO undertook an effort to improve the cyber security of their 100,000 desktop computer network. They focused on three areas: putting in place continual monitoring of their networks, developing a template and collecting audit data for building risk measures for each network, and publishing the results across the DOS to allow the sharing of best practices and using peer pressure to drive low performing network owners toward improvement.

While the DOS system is certainly simpler than DoD's, many of the barriers they had to overcome: culture, use of technology, and the development of standards and

templates to create a common language used to address issues across the department, were very similar.

DOS started with five objectives:

- Scan every 36 to 72 hours
- Focus on attack readiness
- Find-fix top issues daily
- Grade personal results
- Hold managers responsible

Figure 8.1 below shows an example scorecard for a network segment from the DOS network assessment process.

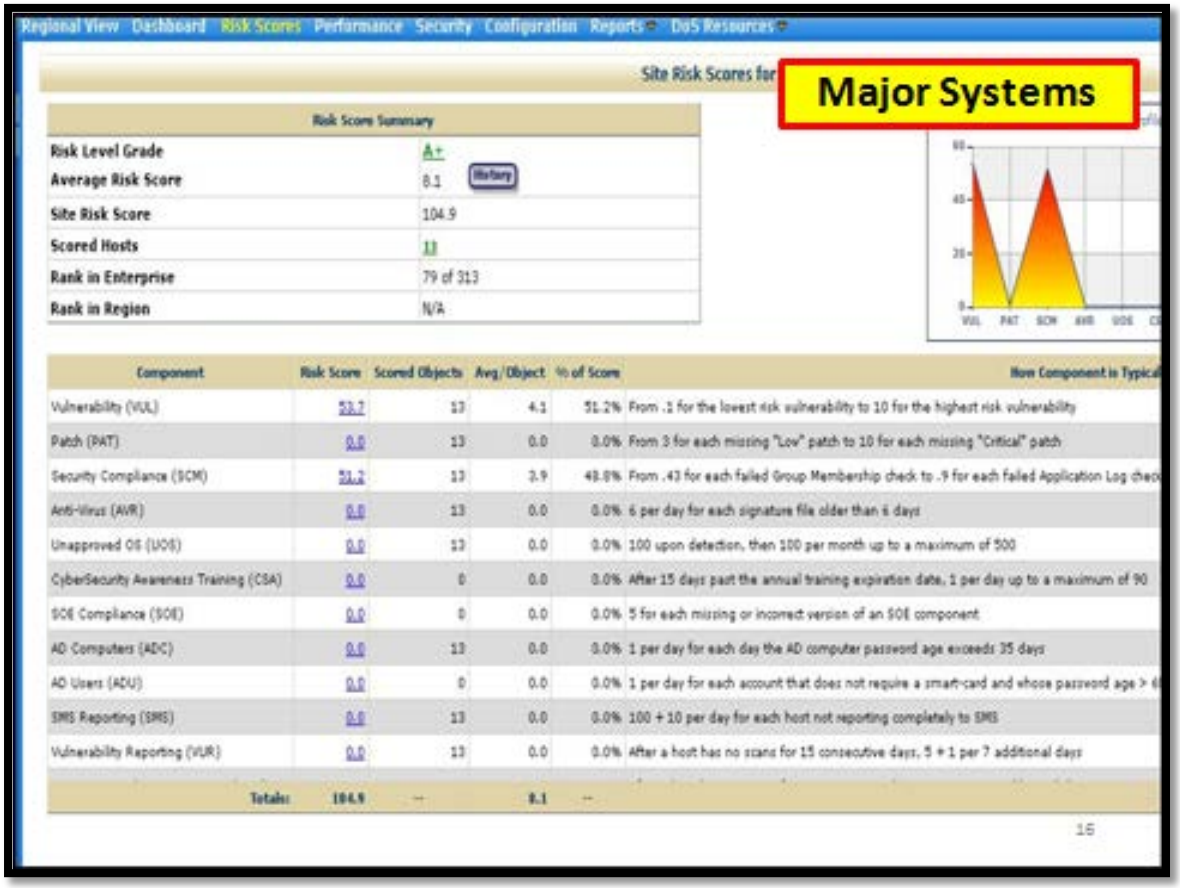

Figure 8.1 DOS System Risk Scorecard

The data from the scorecards for each network segment are then aggregated into an enterprise view as shown in Figure 8.2. This level of data aggregation allowed DOS senior management to identify risky portions of their broader networks and to focus resources on those areas. While

the DoD should develop its own methods and processes to deal with its enterprise, the DOS example is a good reference point.

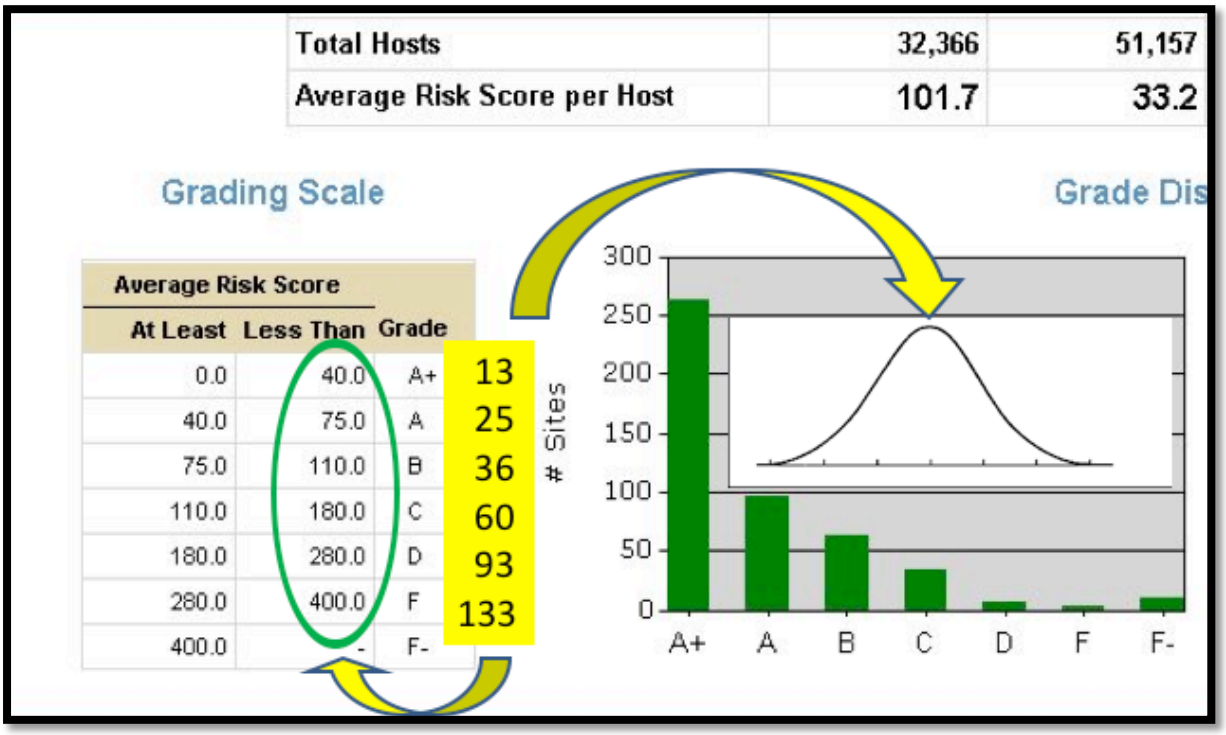

Figure 8.2 DOS Risk Score Indicator for Enterprise

As a minimum for DoD, continuous monitoring of networks should be expanded to touch all elements with continuous scanning. Audits should be conducted on a regular basis (every 12 to 18 months) on each network segment. The output from the audits should be used by the Secretary of Defense and DoD CIO to improve weak performers toward "green" status and to identify and share best practices across the DoD. ***The results of the audits should become part of a commander's readiness assessment for their operational systems.***

One particular challenge for the DoD is the number of networks and systems that contain technologies no longer supported by the commercial sector. Those systems must be identified and either updated and brought into compliance (preferred, but may not be affordable), or re-positioned in separated enclaves from the broader GIG; connection to these systems should pass through strong firewalls and sensors at CIO controlled points. Permitting out-of-date systems to remain connected to the broader network without the strong controls at access points will only continue to offer attractive vulnerabilities for attackers to exploit.

8.2.1.5 Build Network Recovery Capability

It is not unusual for a sophisticated adversary, who has infiltrated a network, to monitor in real time as the network owners try to kick them out. Frequently, the adversary then implements a counter to the network owner's defensive actions and

can be back in the network in a matter of minutes or hours. To fight and win in a war that includes cyber capabilities, DoD can't afford to have the enemy inside its control loops. If DoD is in that situation, then it needs backup (war reserve) mechanisms for C2. Less critical systems need the ability to communicate over an alternative system to address network intrusions, forcing an adversary to penetrate multiple systems and be able to operate both in an integrated, real time fashion to track DoD counterattacks as we try to regain control of our network or system. Having the ability to gracefully degrade and maintain the most critical functions of the systems at an operational level is highly desired, and can usually be achieved with lower bandwidth links.

8.2.1.6 Recover to a Known (Trusted) State

The goal for DoD operational systems should be to:

- Develop the ability to know (and report) if the network or system has been penetrated,
- Gracefully degrade or have provision for alternate mechanisms to continue the most critical mission functions and
- Recover eventually to a known (trusted) state.

Earlier recommendations addressed the first two goals. The last goal is perhaps the most challenging. While maintaining a "gold copy" of system operating software (including firmware, etc.) seems straightforward, a sophisticated adversary will implant an attack into the system via stealthy means. If the adversary has enough patience, as operating systems are updated and gold copies evolve, the adversary's implant will migrate and become part of the trusted baseline. Should a future attack be executed and disable the system, restoring the gold copy software would only reinsert the adversary's original implant.

The Department must develop methods to evolve trusted copies of operating software for systems that ensure only the desired changes are made in the gold copy. Tools exist to perform code checks and are currently used in some important systems (e.g., strategic fire control systems). However, these tools require substantial amounts of human interaction and thus would be difficult to employ broadly across DoD systems. The Department should continue to search the commercial and contractor space to develop tools with higher levels of automation for this function.

Note that these efforts may still be insufficient to protect against an opponent that has operationally introduced vulnerabilities at the hardware level. However, for low- and mid-tier threats, properly executing these measures would significantly enhance DoD's defensive posture.

8.2.2 The DoD should leverage commercial technologies to automate portions of network maintenance and "real-time" mitigation of detected malware.

- Build on existing tools and capabilities currently in use
- Automate response to threat conditions
- Leverage cyber ranges to test emerging technology and develop tactics, techniques and procedures (TTPs) and guide investment strategies.
- Develop mitigation/transition plans for legacy systems

- Responsibility**:** DoD Chief Information Officer, with support from NSA-IAD, IOC: 6 months, with enhancements released on a quarterly basis

As discussed above, modern COTS software has dramatically improved and can provide automation of several key network management functions. The software products sit at the firewall and behind the firewall which is particularly important to find and track advanced persistent threats. Table 8.1 below includes examples of technologies currently available in the commercial markets and highlights benefits that they offer. The Task Force has been careful to not recommend any products by name or endorse any specific vendors.

Table 8.1 COTS Technology to Automate Portions of Network Management

Technologies Available as COTS	Benefit	Threat Level Addressed
Enhanced server and network device configuration management.	Automated detection of the status of servers and communications equipment has been refined to a science. New tools are available to dramatically enhance system hygiene through monitoring state and automating patch management. Benefit is enhanced resiliency and better ability to rapidly recover to known best state.	Tiers I, II
Mobile device configuration management	Enhances ability to manage mobile devices through enterprise tools.	Tiers I, II
Mobile device sandboxing of enterprise data and apps, including virtualization of enterprise desktops	Key to preventing information loss via lost or compromised mobile devices.	Tiers I, II, III
Cloud server security platforms with file integrity monitoring, dynamic firewall automation, configuration monitoring/management, vulnerabilities assessments all optimized for cloud capabilities	Establishes a means to test configuration and manage capabilities provided by public clouds and even internal private clouds shared by internal organizations.	Tiers I - IV
Automation of content distribution and control of content enabling fine-grain tracking of who is authorized to receive and read content.	Mitigates some information disclosures.	Tiers I - IV
Advanced log and event sense-making solutions including analytic approaches for bringing all the data	New Hadoop-based capabilities are enabling enhanced information fusion including sense-making over incredibly large data sets, providing	Tiers I - IV

Technologies Available as COTS	Benefit	Threat Level Addressed
together for analysis.	benefits of enhanced knowledge of adversary activities.	
Enhanced browser sandboxing to prevent hostile code from entry into the enterprise via the browser.	Significantly reduces the ability of adversaries to trick users to download hostile content or to click on a link that points to a site with malicious code on it.	Tiers I - II
Enhanced configuration management enabling tracking all known state variables to determine device compliance and normality and in real time return systems to known state.	Support to automated hygiene, enhanced defense and more rapid restoration after attack.	Tiers I - IV
Enhance network analysis and real time rule based decisions over traffic at line rates.	Assessment of damage from attacks and continuous hygiene monitoring. Ability to create and update millions of rules on a single device will provide dramatic flexibility in creating new enclaves, blocking communication with hostile sites and preventing malicious code from entering. Will also mitigate key data exfiltration threats.	Tiers I - IV

While these technologies do not address Tier V-VI threats directly, when properly deployed, they make an attacker's task of moving data throughout the systems, while remaining undetected, much more difficult. Our goal is to raise the costs for the Tier V-VI attackers to succeed, limiting the number of operations they can afford to attempt.

8.2.3 USD(P&R), in Collaboration with the DoD CIO and the Service Chiefs Establish a Formal Career Path for DoD Civilian and Military Personnel Engaged in Cyber Defense

- Address training and certification requirements
- Define career designations
- Define incentives for personnel achieving higher levels of certification
- Ensure that there is a cadre of high end practitioners
- Completion: 18 Months with quarterly reviews with the DEPSECDEF

The Task Force expects cyber-focused personnel to move between offensive and defensive focused posts throughout their career. The best defenders will be those who understand what can be accomplished from an offensive point of view (the reverse is also true). Creating cyber warriors with expertise in offensive and defensive cyber skills should be encouraged. In fact, the Task Force anticipates a greater use of our offensive capabilities to support defensive objectives.

8.3 Cyber Defense (Hygiene) Performance Measures

How DoD defends its systems is perhaps the most straightforward area in cyber to apply useful measures. Most successful attacks reaching DoD networks today result from a personnel failure or out-of-date software in firewalls and detection systems. Most of these attacks are understood and preventable through known signature management (patching), yet DoD defensive systems don't keep up, and attacks continue to penetrate DoD's networks. The architecture and standards to be defined by the DoD CIO in the earlier recommendation provide a starting point toward improving the Department's cyber network defensive posture. A key element for success is driving compliance through the Department. The independence taught to DoD military commanders that provides such significant benefit on the battlefield is a risk to the Departments networks as systems become more and more inter-connected. Relative to cyber, the impact of risk decisions the commanders make in the field is no longer contained within the local environment. To drive the needed behavior, audit results from the CIO must be published and consequences imparted on those consistently out of compliance.

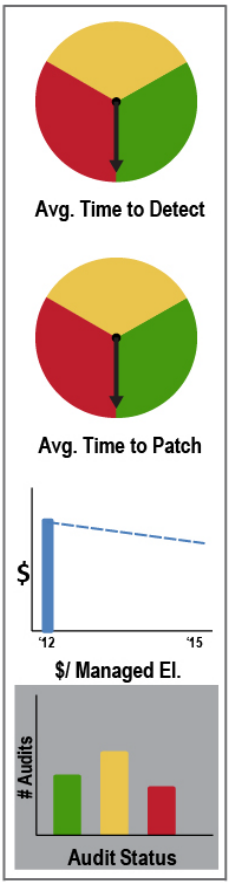

Figure 8.3 Cyber Defense Hygiene Performance Measures

Notional cyber defense hygiene performance measures are depicted in Figure 8.3. The first proposed measure is of the number of audits conducted. The results of these audits can be illustrated on a red-yellow-green scorecard. Corporate examples of this practice allow an organization time to move a yellow audit to green by the next audit cycle (typically annually). Red audits require a plan to move the network to green status in a shortened timeframe and are reported to the CEO and the audit committee of the Board of Directors. The same level of leadership attention is required to ensure the importance of compliance to cyber security standards is understood throughout the DoD.

One of the benefits to each network operating organization conducting CIO-directed audits, will be achieving a higher fidelity inventory of the types and quantities of devices connected to its network. Once those inventories are available, along with the budgets to operate the networks, DoD can produce metrics on the cost to manage a "network element". Collecting this data across DoD networks will provide a basis for comparing network architectures and the actual cost to operate them. This information can be used to identify best-in-class performance within the DoD structure and to drive greater efficiency over time across the broader structure.

The Department would ultimately like to know "who" is in its systems, how they got in, and how long it took DoD to get them out and restore the systems to full operation. To prepare the Department to gather these measures in the future, DoD needs to first understand more about the basic components that drive system vulnerability and develop an ability to detect attacks. Therefore, the next proposed measure is a rollup of the average time to patch a system from the time a software update for a specific attack (signature) becomes available. This report recommends relocating this activity away from manual interaction by network operators to

more automated capabilities. As automation levels are increased, the time-to-patch duration should drop precipitously, speeding protection against some (known) attack. The final measure is the average time to detect an attack that has successfully penetrated the network. As successful attacks are found in networks, forensics should be conducted to understand how the attack penetrated and propagated through the network. Gathering information to understand how attacks entered the network and how long they have been sitting in DoD networks marks the beginning toward an understanding of the Department's ability to actually detect and remove successful attacks. It also becomes a measure of how advanced its cyber hunting skills on the network have become as more of the mundane functions are automated and more resources are turned toward ferreting out anomalies within network logs and operations. As more advanced log management tools are deployed on the network and more resources dedicated toward hunting on the network, the time that an attack resides within the network should drop. This data would provide a basis to understand how attacks get into the network, how well we find them and how long it takes to reestablish trust in our systems.

9.0 Changing DoD's Cyber Culture to Take Security More Seriously

9.1 Background

DoD's Cyber Culture: Operational Necessity and Personal Culture-Leadership faces an immense challenge to change DoD's culture regarding cyber and cyber capability. Individual and organizational cyber practices result in so many cyber security breaches that many experts believe that DoD networks can never be secure with the current cyber culture. The individual's immersion in the civil sector cyber culture and the military's focus on mission objective are the two most important contributors to DoD's poor cyber culture. In the face of a threat that routinely exploits organizational and personal flaws, DoD leadership must develop a clear vision for the Department's cyber culture.

Most DoD employees, both military and civilian, learned to use the Internet and network capabilities long before they became DoD employees. The naive acceptance of trust in their personal Internet use, and increasing expectation of 24/7 access establishes the baseline for the individual's experience with IT. Little to no thought is given regarding the implications of the vulnerabilities of these personal computing platforms (e.g. smart phones, cameras, printers, etc.). While there is an increasing awareness of personal cyber vulnerability (e.g. identity theft, stolen passwords, etc) and a slowly evolving corresponding acknowledgement of the need for increased security requirements, most problems have not resulted in repercussions serious enough to change behavior. There is very little personal accountability maintained in the civil cyber environment and the consequences of risky behavior is generally marginalized (e.g. the majority of individuals still use predictable and/or easy to crack passwords). Returning to the simpler, more secure non-networked days to solve this problem is an unreasonable expectation and the individual's ability to undermine effective defensive measures cannot be over stated. Since personal cyber practice will potentially trump any rules DoD attempts to impose on its workforce, DoD leadership must take significant steps to educate and impose accountability on individual cyber behavior.

Military culture thrives on overcoming barriers to achieve mission objectives, leaving cyber security, at best, a second thought for even knowledgeable commanders. A common refrain from operational commanders is "Better to be judged by twelve than carried by six." While mission objectives can and should take primacy, commanders must realize the implications of cyber security compromise. A simple tactical expedient in the most remote theater of operations can, under certain circumstances, create a strategic vulnerability elsewhere in the world. However, this is not the first time commanders and political leaders were forced to make disciplined decisions trading tactical objectives against strategic capability. The United States and UK exploitation of ULTRA in World War II often traded short term gains for long term strategic objectives. ULTRA exploitation was so sensitive that it was not officially disclosed until 1974, almost 30 years after the end of WW II.

Additionally, few commanders know or understand the intricate network of devices, hardware, and software that provide them the combat capabilities they depend on to accomplish their

missions (e.g. Deputy Secretary Lynn's article "Defending a New Domain"), nor the tools and techniques that are required to infiltrate their systems some as simple as access control. For example the Task Force received a briefing that provided an account of the same individual providing red team member's access via the same known vulnerability two years in a row. Especially worrisome, the individual in question complained to the testing team in year two about the lapse in year one. The individual's failure to address personal shortcomings and the Command's failure to hold its individuals responsible for cyber security in the most routine tasks creates untold vulnerabilities easily exploited by any tier threat.

Communicating Change: Absent strong leadership, individual and organizational behavior are unlikely to change from the permissive and open environment we experience in our personal lives. Senior DoD leadership must communicate a new vision of cyber excellence to the entire Department. This challenge is not new. The U.S. military is one of the best organizations in the world at driving culture and compliance when it chooses. DoD possesses robust cultures impacting physical fitness, weapon control, and handling of classified material-- all communicated by leadership and supported by policy, processes and procedures, training, and breach response actions that strongly reinforce policy to include penalties and loss of privilege that result in loss of employment or prison. In some of the programs mentioned above, achieving compliance required removing the local commander's discretion (e.g. continued failing of weight standards or the physical readiness test will result in dismissal no matter how well the individual performs in all other aspects of their job). Clear expectations of the consequences and mandatory reporting of objective measurements created the environment to drive behavior in the desired direction.

To implement the Department's leadership vision, DoD must develop and apply similar disciplined approaches of personal and command accountability for cyber actions. Leadership must establish policies, standards, and expectations for secure use of DoD networks and systems. While implementation of some cultural practices allow for local command discretion, the cyber threat is too serious. Policies, standards, and expectations must be consistent and not be optional.

To support culture change, leadership focus must provide effective, consistent and sustainable training and education programs. Too much of DoD's required cyber training is a static, check-the-box drill. DoD needs to develop training programs with evolving content that reflects the changing threat, increases individual knowledge, and continually reinforces policy. Training and education programs should include innovative and effective testing mechanisms to monitor and catch an individual's breach of cyber policy. For example, DoD could conduct random, unannounced phishing attacks against DoD employees similar to one conducted in April of 2011 by a high tech organization to test the cyber security awareness of its workforce. Within a one week period the organization's CIO sent a fake email to about 2000 of its employees. The fake email appeared to originate from the organization's Chief Financial Officer and warned the employees that the organization had incorrectly reported information to the Internal Revenue Service that could result in an audit of their tax return. To determine if they were affected, they were asked to go to (click) to a particular website. Almost 50% of the sample clicked on

the link and discovered that this had been a cyber security test. Each of them had failed. Had this been a real phishing attack, every one of these employees not only would have compromised their machines but would have put the entire organization at risk.

Following an initial education period, failures must have consequences to the person exhibiting unacceptable behavior. At a minimum the consequences should include removal of access to network devices until successful retraining is accomplished. Multiple failures should become grounds for dismissal. An effective training program should contribute to a decrease in the number of cyber security violations.

Exercises provide another mechanism to increase effectiveness in an increasingly diverse and hostile cyber environment. Numerous DoD components use realistic exercise programs to increase operational proficiency. Similar techniques must be developed and applied to DoD components and enterprise. Exercise realism should grow from year to year to ensure the DoD closes the cyber threat vulnerability gap.

Today, information assurance and mission assurance are inseparable – as such, command readiness should assess and include cyber policy compliance. Established in 1999, the Defense Readiness Reporting System provides a broad assessment of personnel and systems related to the successful execution of DoD missions. The current DoD Directive (DoDD 7730.65, certified current as of April 23, 2007) provides readiness criteria for virtually every element of war fighting capability, including personnel education, training, and proficiency testing. There are measures to assess Commanders on unit fitness to execute assigned missions and penalties for failure to meet specific standards. Nowhere in the readiness structure are there criteria that specifically addresses the performance of IT components critical to the successful execution of the mission. Reflecting on BUCKSHOT YANKEE, the infection was (likely) caused by a well-intentioned service member who violated policy by moving a flash media device between the unclassified and classified domains. This action resulted in severe impacts on operations and literally months of recovery by individuals already overextended with their normal duties. While this was one of the most egregious examples, any Tier II Computer Network Defense Service Provider (CNDSP) will readily admit that infection of the classified networks due to the inappropriate use of media devices occurs on an all too regular basis. Absent accountability, the situation will never change. Today's permissive cyber culture allows personnel to violate cyber policy in order to get the local job done. These local decisions frequently put the enterprise at risk and as a consequence, mission assurance at risk.

9.2 Recommendation: Change DoD's Culture Regarding Cyber and Cyber Security.

9.2.1 Establish a DoD-wide policy, communication, and education program to change the culture regarding cyber and cyber security

Secretary of Defense, Chairman, Joint Chiefs of Staff and their direct reports communicate a vision of DoD Cyber Security for 2020. Secretary of Defense and CJCS provide direct communication to all organizational elements explaining the threat and consequences of cyber actions is essential to change DoD's cyber culture. Leadership must change the

current culture which is focused on an overwhelming emphasis on operational objectives and shaped by daily exposure in civil cyberspace that imposes little cost to risky behavior.

- Commander, USCYBERCOM and the DoD CIO establish a plan with measureable milestones and flow down to all organization elements. The plan must comprise:
  - The policy, operational rules, and expectations for secure use of DoD networks & systems
  - The training program and follow on continual reinforcement of the policy
  - A small "tiger team" of experts to monitor, test, and catch breaches in policy
  - Clear punitive consequences for breaches of policy

DoD must develop training that evolves with the threat and increases individual knowledge. Training failures must bring consequences, including removal of access to network devices until successful retraining is accomplished. Multiple failures should become grounds for dismissal.

Commanders should use exercises as opportunities to test cyber-hygiene. Realism in exercises should grow over time to ensure operational forces are resilient in the face of an evolving cyber threat.

- Following the education period and a short grace period, penalties should be imposed similar to the breach of policy for classified material

- Command readiness should assess and report cyber policy compliance. SECDEF should require the policy to be communicated within 60 days and the education and roll out to every DoD and contractor employee in 9 months.

The current DoD Directive (DoDD 7730.65, certified current as of April 23, 2007) must be modified to include readiness criteria for cyber capability. Specific performance measures related to the IT components critical to the successful execution of the mission must be used to assess Commanders on unit fitness to execute assigned missions and the readiness system must incorporate penalties for failure to meet specific standards.

9.3 Cyber Culture Performance Measures

The cultural aspect of developing an understanding of the importance of proper cyber hygiene and conduct will probably be the most difficult to achieve activity recommended in this report. It requires changing perceptions and history of how military and civilian personnel are taught to operate. Cyber culture must become as important as weapons handling or physical fitness to our military service members and DoD personnel (and the contractors who support them). Only two performance measures are proposed in this section (Figure 9.1). Each is very simple and consists of easily gathered data. The first is the percentage of the total population to complete the DoD Cyber education program. The green level for the measure should be set very high (above 99%) and the Secretary and his/her direct reports need to take an active ownership role

and participate in this education program to ensure ***every*** DoD person has the mandatory training.

The second measure is cyber security violations, rolled up across the Department, and on the same chart the number of punitive actions that have been taken as a result of those violations. Until there are well understood and supported consequences for violating cyber security policies, cyber security will never be viewed as important across the Department.

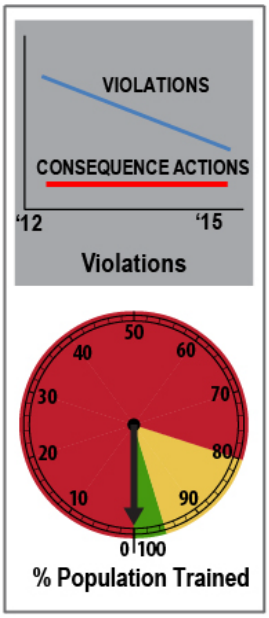

Figure 9.1 Cyber Culture Performance Measures

10.0 Building a Cyber Resilient Force

10.1 Background

Creating a cyber-resilient force in a cost effective manner will challenge DoD. The cyber threat's pernicious intrusion into every aspect of DoD, and its support community, create a global exploitation opportunity for any adversary willing and able to discover or create vulnerability. Fortunately, DoD's experience in building its nuclear deterrent forces provides a proven model to achieve a cyber resilient force (segregation, inspection, trusted suppliers, etc.).

10.1.1 Building a Cyber Resilient Force: The fundamental purpose of building a cyber resilient force is to achieve mission assurance in the cyber environment. Achieving affordable mission assurance, especially against high tier threats (V-VI), requires discipline to first identify protected-conventional capabilities that the United States can rely upon in a cyber attack and then to segment specific forces that will be used to accomplish desired missions. Only these forces receive the highest degree of cyber resilience necessary for assured operation in the face of a full spectrum adversary. This protected-conventional capability, combined with offensive cyber discussed in Chapter 7, form the rungs of an escalation ladder with nuclear forces at the top. To achieve a high degree of cyber resilience at an affordable cost, the Department must segment and segregate the force structure that deliver the desired capability in response to a cyber threat.

As mentioned previously, segmentation must differentiate only those forces required to achieve the desired mission and is not required across an entire capability. This will require a different way of managing the capability. (For example, designating 20 aircraft by tail number as cyber resilient, out of a fleet of hundreds, segregated and treated as part of the cyber critical survivable mission force.) Segmented forces must remain separate and isolated from the general forces, with no dual purpose missions (e.g. the current B-52 conventional nuclear mission). Segmented forces can be used in regional and theater cyber conflicts as a standalone cyber-resilient capability.

Once specific systems are identified, they must be brought to a known cyber resiliency standard which can be used to design, build and measure capability against. The standard must evolve as the cyber threat changes but the Task Force identified a set of attributes for consideration:

- Return to a TRUSTED, known state. The known state must be time invariant. Failing this, components must be controlled throughout their lifecycle and segregated from general purpose forces, including use of and connection to general force networks;
- Maintain component awareness/control (e.g. sensing and reporting of buffer overflow conditions and bit parity checks, reporting and control of update/file transfer points (e.g. USB ports), real time or near real time monitoring at the component level to ensure installation of authentic components/software);

- Maintain network awareness/control (e.g. installation of sensing points to measure network performance and patterns, trusted log audit capability, and trusted and automated patch/update capabilities);
- Provide operational environment support (e.g. identify conditions under which a system can be connected to specified network, conditions under which it must be disconnected or operate in a degraded mode such as use of an out of band path that supplies x% of the unfettered capability, and recovery mechanisms).

Once developed, the standard should inform the requirements process which would allow the operational community to know what it is asking for and also what it is receiving. In addition, a subset of the resiliency standard should be applied to the rest of the force structure at every opportunity to incrementally raise the overall cyber resiliency of DoD. Development and application of a resiliency standard will help tell what DoD is building, but DoD must also focus on how it will accomplish mission assurance.

10.1.2 Subject Defined "Cyber Critical Systems" to More Stringent Mission Assurance Activities: The bottom line objective of system resiliency is assuring mission execution. Therefore, the designated systems must be subjected to a mission assurance assessment process depicted in Figure 10.1 that is structured around a knowledgeable workforce, incorporates feedback from every available means, conducts research and develops new technology addressing cyber resiliency issues, and manages life cycle integrity.

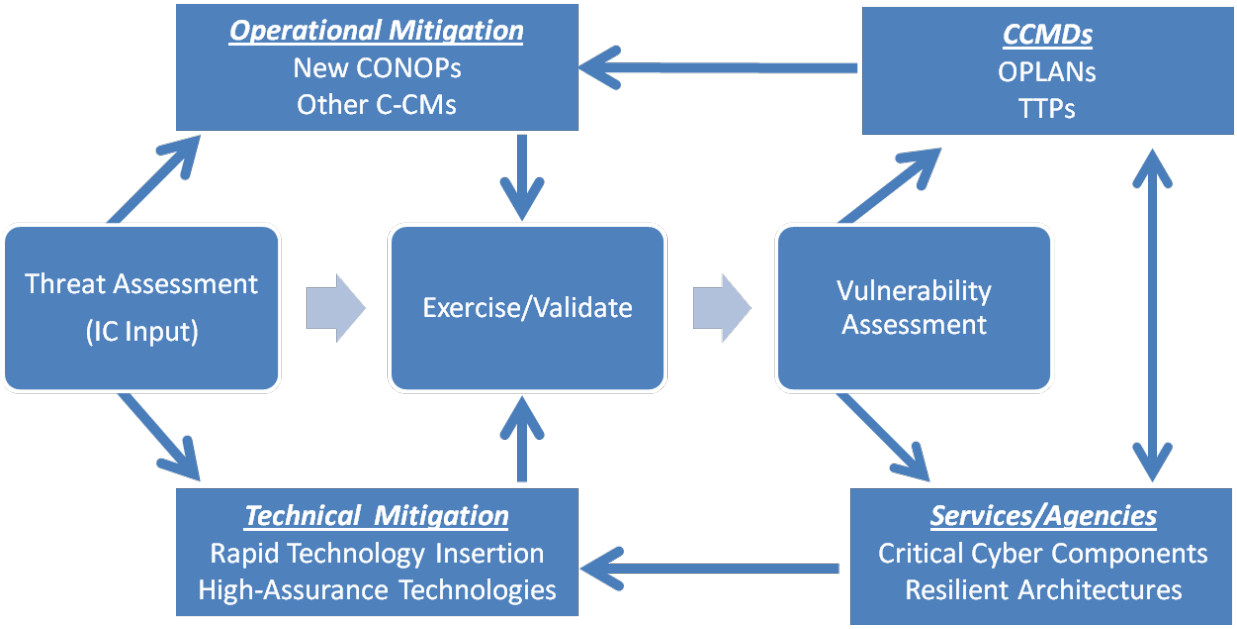

Figure 10.1 Mission Assurance Assessment Process

The study team could not identify any instances where mission-based analyses were being routinely and systematically used to enhance cyber resiliency. However, there is recognition within DoD of the need for such assessments; for example, the working group under the DoD Cyber Integration Group charged with the task "develop and implement resilient, defensible cyber environment" is promoting activities that would lead to such assessments.

Enhancing Operational Feedback: As mentioned above, success will require operational know-how. While the current level of cyber activity develops a cache of experience and operational know-how that can be applied to the workforce, there are gaps at all levels (tactical, operational, and strategic) due to the newness and current compartmentalization of cyber operations. Lacking a full scale cyber war, the development of U.S. nuclear deterrent forces again provides a good model for obtaining operational knowledge in the cyber environment. Specifically, the Department should develop/expand opportunities, including enhanced ability to feed to/from operational exercises (e.g. CCMDs, Services, joint operations) and the testing community, developing sophisticated modeling and simulation capabilities, utilizing inputs from the intelligence community, and building partnerships with the private sector that provide information of the operational cyber environment to be applied to building cyber critical survivable mission force components.

The Department is moving in this direction. For example, in February 2011, Chairman, Joint Chiefs of Staff issued an instruction[36] to incorporate realistic cyberspace conditions in major DoD exercises. In response to the Instruction, exercise planning has begun to address these realistic conditions and most notably to understand and redress the shortcomings.[37] While these efforts offer promise, they need to be developed into a more comprehensive and systematic approach to fully address the mission assurance limitations and meet the intent of the Instruction.

10.1.3 Developing the Cyber Work Force: Developing and meeting standards and requirements will require a technologically competent cyber workforce. The workforce must be capable of providing disciplined system architecture, engineering expertise and operational knowhow capable of specifying buildable, measureable, and testable systems that support the overall realization of cyber resiliency. Developing an ability to correct known (Tier I-II) vulnerabilities in complex, interconnected systems requires both a global perspective (not typically present at the Program Manager level) and technical expertise at the Component level.

Developing a capability to rapidly respond to the discovery of new vulnerabilities (Tier III-IV) requires implementation of new concepts in the requirements, acquisition, testing and operational communities. Success against the Tier V-VI threats (causing frustration and additional cost for the attackers) will require informed decisions balancing operational objectives and technical performance--to include out-of-band communication capacity and degraded modes of operation in the cyber environment.

[36] CJCSI 6510.01F: Information Assurance and Support to Computer Network Defense, 9 February 2011
[37] DoD 8570.01-M; Information Assurance Workforce Improvement Program, December 19, 2005

The technical cyber workforce must work across the capability lifecycle. Standards and requirements are addressed above but the Acquisition Community (e.g. Development Centers, Depots and industrial partners) bears a significant responsibility in this endeavor. DoD systems are acquired through development centers with responsibility for specific mission areas (e.g. space systems, aircraft, ships, C2 systems, etc.). Since virtually all DoD systems use cyber components in increasingly critical roles, all development centers must engage the cyber security challenge. Depots are charged with maintenance and updating of substantial components of the DoD infrastructure and will be targeted by those seeking to compromise the DoD cyber capability, just as are the other elements of the system lifecycle infrastructure. Industrial partners that produce DoD systems must also address the cyber threat.

10.1.4 Development of Secure System Technology: In addition to failures in cyber hygiene and in tepid response to exposed cyber shortcomings and transgressions, it is clear that the DoD and its community do not possess tools to produce and operate systems at a high enough level of cyber integrity. One potential architectural solution is identified by the other component of the DSB Cyber initiative, the *DSB Task Force on Cybersecurity and Reliability in a Digital Cloud.* That Task Force examined the applicability of cloud architecture to DoD uses. That study determined that a well-architected cloud significantly enhances the ability to deal with known Tier I-II vulnerabilities and could provide advanced analytic capability to mitigate Tier III-IV threats. However, the study acknowledges that today's cloud architectures are not applicable to all DoD systems (e.g. nuclear command and control) and will not address legacy systems, therefore other solutions are required.

The DoD science, technology and engineering community must engage with those in academia, government laboratories, and industry working innovative cyber technologies, processes and disciplines needed to raise the level of our national competency and capability in secure systems. System security engineering is a discipline that needs particular attention, and can be a bridge between the engineering and IT communities. Areas to be pursued in the longer term include: development of special purpose system architectures with inherent resilience, systematic analysis of potential modes of cyber vulnerability of systems, use of emerging technology developments for system resilience, such as trust anchors, minimal functionality components, simplified operating systems, developing a means to verify compromise of fielded systems contributing to critical missions, creating trust in systems built with un-trusted components, and restoring to a known state ("gold standard").

Addressing Infrastructure Vulnerabilities: Although not specifically tasked to examine infrastructure vulnerability, it became readily apparent to the Task Force that infrastructure is vulnerable to the cyber threat. The Task Force identified some areas of technology for rapid development that potentially increase the cyber security of critical infrastructure systems.

Similar to previous DSB work[38] involving infrastructure vulnerability, DoD's primary interest in critical infrastructure is associated with its force projection capability. However, as discussed in previous chapters, the Task Force finds that a catastrophic cyber attack on the infrastructure poses an existential threat to the nation. Fortunately a number of infrastructure systems (e.g. power systems, water systems, air traffic control systems) share characteristics that could allow better protection from cyber attacks (e.g. relatively few in number, can be operated with modest bandwidth, and can tolerate decision time cycles in seconds instead of microseconds). Potential areas of consideration which need to be addressed to mitigate infrastructure vulnerabilities include:

- Trusted hardware coprocessors with appropriately validated software;
- Techniques to monitor and verify tampering;
- Encryption;
- Reset mechanism through parallel processor;
- Insider protection schemes (e.g. 2-person rule for critical system override).

As long as DoD mission success relies upon infrastructure, it must actively engage in and encourage efforts to reduce infrastructure vulnerability.

10.1.5 Component Sourcing- Intelligence Community Initiate Supply Chain Collection Activity: DoD is in the process of institutionalizing a Supply Chain Risk Management (SCRM) strategy. The strategy prioritizes scarce security resources on critical mission systems and components, provides supply chain intelligence analysis to acquisition programs, and incorporates vulnerability risk mitigation requirements into system designs via engineering and acquisition practices. Component sourcing is an increasingly important contributor to cyber resiliency. An increasingly globalized development and production system supplies the electronic components (hardware, software and firmware) of DoD systems. Production of these "parts", sometimes including customized parts, external to the United States comprises a serious threat vector to the U.S. DoD architecture and systems. If DoD is to improve cyber defense and resiliency of DoD systems, it must better understand the implications of the supply chain for the components of U.S. systems, including the substantial amounts of custom hardware and software developed, deployed, operated and maintained in systems by and for the DoD.

Several approaches exist to address untrustworthy or unprotected sources. Supply chain assessment is an essential component of an overall cyber resiliency approach. However, many tiers in the supply chain (designers, producers, brokers, subsystem suppliers, major system integrators, etc.) limit visibility and make the origins of components difficult to track and certify. DoD's previous use of a trusted foundry program addresses both untrustworthy source issues and also missions requiring such limited number of parts (e.g. radiation hardened components)

[38] DoD Energy Strategy (published Feb 2008); Critical Homeland Infrastructure Protection (published Jan 2007); DoD Roles and Missions in Homeland Security (November 2003).

as to be economically unviable for commercial chip manufacturers. However, trusted foundries are capital intensive and present challenges with ensuring the broad spectrum of DoD microelectronics needs, which span generations of technology as well as leading edge. Fortunately, market forces provide an economic incentive to some companies to pursue cyber integrity of their products. DoD will need to share best practices with these same companies as part of its resilient force buildup.

10.2 Recommendation: Build a Cyber Resilient Force.

10.2.1 DEPSECDEF should direct specific actions to introduce cyber resiliency requirements throughout DoD force structure.

10.2.1.1 The DoD CIO, in coordination with USD(AT&L) should establish a resiliency standard which can be used to design, build and measure capability against. The Joint Staff will use the standard to inform the requirements process.

Realizing that the standards are likely to evolve as the cyber threat evolves, the Task Force identified certain characteristics that the Department should address as it develops the standards and requirements for cyber resiliency to apply to key conventional force capabilities designated as components of the escalation ladder described in Chapter Five. These include:

- Until a return to a TRUSTED, known state capability is developed, the forces and capability components providing a cyber critical survivable mission must be controlled throughout their lifecycle and segregated from general purpose forces, including use of and connection to general force networks. Segregation must provide sufficient capability to provide a credible component of the escalation ladder yet not be so large as to create a resource black hole.
- Maintaining component awareness/control is an important feature of resiliency. Desired awareness measures include sensing and reporting of buffer overflow conditions and bit parity checks, reporting and control of update/file transfer points (e.g. USB ports), and in the future--real time or near real time monitoring at the component level to ensure authentic components/software are installed.
- Maintain network awareness/control. Install sensing points to measure network performance and patterns, develop and maintain trusted log audit capability, and incorporate trusted and automated patch/update capabilities.
- Support the operational environment such as the conditions under which a system can be connected to specified network, conditions under which it must be disconnected or operate in a degraded mode (e.g. using an out-of-band path that supplies x% of the unfettered capability), and recovery mechanisms.

The Department must write achievable and testable requirements. For example, establishing a requirement that "System X" must be protected against a Tier III-IV threat will force the test community to engage in an infeasible activity as they are

forced to certify a system against undiscovered vulnerabilities. The Task Force is wary of the efficacy of establishing a resilience "ility" to work in the same trade space as other "ilities". This approach tends to be bureaucratic and prior to adoption, must demonstrate real effectiveness against the cyber threat.

10.2.1.2 Apply the cyber resiliency standard to the segmented force identified as part of the escalation ladder described in Chapter Five.

In the absence of a cyber threat, the segmented forces are likely to possess slightly less capability than their non-segmented counterparts due to the isolation from every part of the supporting infrastructure which generates so much advantage to DoD. However, in the face of an adversary employing cyber, the segmented forces will provide far more capability than the non-segmented counterparts.

Subsets of the cyber resiliency requirements for cyber critical survivable missions should be incorporated into the rest of the force structure to defend against Tiers I/II, mitigate the effects of Tier III-IV attacks, and drive up the costs for Tier V-VI attacks.

10.2.1.3 Increase feedback from testing, red teaming, intelligence community, and modeling and simulation as a development mechanism to build out DoD's cyber resilient force (USD(AT&L), USD(I), DOT&E, SAEs, CJCS)

DoD must ensure feedback from these exercises impacts system designs, upgrades, CONOPs and TTPs. Lacking a full-scale cyber conflict, DoD will struggle to understand the full implications and effects of the cyber threat. DoD must fight through compartmentalization, understand a nascent but significant capability with limited real operational experience, and avoid typical first adopter mistakes to maximize its resiliency while retaining the huge advantage gained through the networking. The feedback mechanism will also aid the creation of processes to inform development efforts for new and evolved cyber threat vectors.

10.2.1.4 For programs not part of the segmented force, provide a cyber standard set of requirements (expected to be a subset of the critical program requirements list) to be applied to all DoD programs (USD(AT&L), DoD CIO, SAEs))

The DoD CIO, in coordination with USD(AT&L) should establish a subset of the resiliency standard developed above which can be applied to the rest of the force structure. The subset should be applied at every available opportunity (e.g. new starts, refurbishment, and repair). Legacy systems unable to meet the standard should be isolated or replaced.

The Department must still discipline itself in its application of the subset of resiliency standard to the rest of the non-escalation ladder components. Not every capability must protect against a Tier III-IV threat but all must defend against a Tier I-II threat.

In addition, initial incorporation of the subset of the resiliency standard is likely to require dedicated management to identify and overcome the issues with implementation. The Task Force urges the Department to apply the initial subset of resiliency standards to ACAT 1 programs. Once experience is gained, the resiliency standard can be applied across the Department.

10.2.1.5 Develop DoD-wide cyber technical workforce to support the build out of the cyber critical survivable mission capability and rolled out to DoD force structure (USD(AT&L), CIO, SAEs, DOT&E, USD(I), USD(P&R)).

The technical cyber workforce must function across the capability lifecycle. Similar to the requirements to develop and attract the correct level of cyber talent for DoD's offensive and defensive missions, USD(P&R) must develop supporting policies to build the cyber workforce. The Acquisition Community (e.g. Development Centers, Depots and industrial partners) bears a significant responsibility in this endeavor along with the operational forces, test community, and scientific and engineering community. Historically, security functional responsibilities were assigned to security specialists who typically do not possess an engineering background. While not all participants need to be qualified to work at the highest levels, DoD must ensure that sufficient workforce capability exists. Programs for training and certification must be developed or enhanced so that qualifications can be measured and used in personnel and acquisition decisions. Equal attention must be applied to develop expertise to address system security during design, manufacturing, and sustainment phases of the lifecycle, with particular attention paid to controlling and limiting opportunity for malicious manipulation of components.

10.2.1.6 The Science and Technology community should establish a secure system design project with FFRDCs, UARCs, academia, commercial and , defense industry (ASD R&E, Initiate in FY13; four-year research activity).

The DoD science, technology and engineering community must engage with those in academia, government laboratories, and industry working innovative cyber technologies, processes and disciplines needed to raise the level of our national competency and capability in secure systems. Areas to be pursued in the longer term include: development of special purpose system architectures with inherent resilience, systematic analysis of potential modes of cyber vulnerability of systems, use of emerging technology developments for system resilience, such as trust anchors, minimal functionality components, simplified operating systems, developing a means to verify compromise of fielded systems contributing to critical missions, creating trust in systems built with un-trusted components, and restoring to a known state ("gold standard").

10.2.1.7 The Intelligence Community should initiate a supply chain collection activity (USD(I), 18 months).

The DoD should assess the end-to-end process by which electronic "parts" and systems are produced by select companies to determine if what is known of the cyber threat vectors, including those in Tier V-VI, is appropriately reflected in the efforts of the suppliers. In addition, there is a nexus between cyber threat and relabeled and counterfeit hardware in DoD systems. Both DoD and industry counterfeit mitigation efforts should be developed further in conjunction with DoD cyber defense efforts.

The DoD must similarly assess the software supply chain to gain an understanding of the cyber threat vectors and to understand where mitigation might be possible, practical and affordable. In the parallel DSB study on Cyber Security in Cloud Computing, presentations were received from COTS software suppliers detailing their efforts to create processes for producing high(er) cyber integrity software. DoD should assess best practices in industry for threat mitigation and resiliency engineering, and where appropriate incorporate them into DoD processes and encourage their use in the broader supply chain.

The Acquisition Community must develop partnerships for select capabilities that will enhance the Department's cyber posture. It is generally accepted that the U.S. Intelligence Community possesses the best understanding of the Cyber threat vectors facing the United States. The Intelligence Community must be tasked with specific collection, analysis and reporting requirements on the cyber threat vectors, priorities and activities of U.S. adversaries. Although the Defense Intelligence Agency (DIA) has initiated efforts to provide supplier threat information to the Major Defense Acquisition Program (MDAP) acquisition community, it is not sufficiently broad or mature to serve the needs of critical mission systems. Mechanisms must be developed to share the resulting intelligence assessments, as appropriate, among the significant players in the DoD supply chain and broader national industries.

10.3 Integrated Cyber Requirements Measures

As response to the cyber threat becomes a mainstream component of how DoD operates, it must be reflected in the acquisition cycle used to purchase equipment and systems. Notional performance metrics are depicted in Figure 10.2. The first measure proposed is a simple measure of whether cyber requirements have been included in the acquisition plans and requirements for those systems defined as most critical as part of the conventional deterrent capability. Exactly what is meant by cyber requirements is left to the discretion of the Department. The Task Force envisions such requirements going beyond encryption, storage, and multilevel security, and including requirements to provide sensor points and reporting to better understand if a system has been compromised. For example, if the processor of a system executing activities is not consistent with the expected activities associated with that mission or if buffer register overflows are occurring, etc.

We would expect the same level of requirements, once understood and trialed on the most critical systems, to evolve into the remaining DoD systems, starting first with ACAT 1 programs.

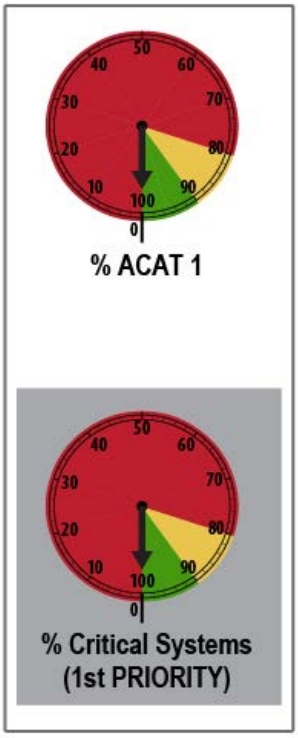

Figure 10.2 Integrated Cyber Requirement Measures

11.0 Order of Magnitude Cost Estimates

The Task Force did not prepare detailed cost estimates for the recommendations in this report. However, due to the fiscal constraints expected in U.S. budgets for the next several years, estimates to the rough magnitude of investment are shown in Table 11.1.

Table 11.1 Estimated Investment Requirements for Study Recommendations

		ROM	Timeframe
1 & 2	Protect the Nuclear Strike as a Deterrent (for existing nuclear armed states and existential cyber attack). Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary.	$$$$	36-60 mo.
3	Refocus Intelligence Collection and Analysis to Understand Adversarial Cyber Capabilities, Plans and Intentions, and to Enable Counterstrategies.	$	12-24 mo.
4	Build and Maintain World-Class Cyber Offensive Capabilities (with appropriate authorities).	$$	12-24 mo.
5	Enhance Defenses to Protect Against Low and Mid-Tier Threats.	$	6-18 mo.
6	Change DoD's Culture Regarding Cyber and Cyber Security.	$	12-48 mo.
7	Build a Cyber Resilient Force.	$$	12-24 mo.
ROM Costs $ <$50M/yr, $$ $50M-$100M/yr, $$$ $100M-$500M/yr, $$$$ >$500M/yr			

Even within a difficult budget environment, much can be done to address challenges faced in the cyber domain. The Task Force believes it is essential that the Department move quickly to better understand the cyber threat and how it relates to national defense and issues of deterrence and escalation. The only recommendations expected to require a large amount of resources are those to ensure the U.S. strategic deterrent is protected to a high degree of confidence and those that build out a protected set of conventional capabilities. While the basic capabilities and components of these systems exist today, understanding and remedying their cyber vulnerabilities, separating their C2 systems and providing backup or war reserve capabilities to ensure available operation in the face of an aggressive attack by a sophisticated adversary, will require time and resources.

11.1 Recommendation: Protect Nuclear Strike, Ensure Availability of Conventional Capabilities

U.S. nuclear capabilities are well isolated and go through regular evaluations of risk against outside forces. Adding analysis and testing against Tier V-VI adversaries is needed to maintain a high level of confidence in the availability of the systems. As the Department considers which systems would make up the ensured conventional strike, there is a range of approaches available to improve the availability of those systems against the cyber threat. Completely isolating systems, redesigning with components from trusted foundries, adding additional

modes for navigation, and fire controls could very quickly lead to costs of billions of dollars. The Task Force feels there are logical compromises that could be made to greatly improve the confidence of system availability during a cyber attack without requiring a total redesign of systems. For instance, focusing some of the capabilities into the submarine force where isolation is already designed into how they operate and fight. U.S. strategic bombers currently use the same air platforms for nuclear and nonnuclear missions. There is a risk due to the broader personnel access allowed during the nonnuclear missions that could impact nuclear missions. Dedicating a number of the bombers to only conduct nuclear or critical conventional missions (as defined in Recommendation 2), and not letting those platforms be utilized for other missions could substantially reduce the risk of cyber compromise of the systems.

11.1.1 Recommendation: Refocus Intelligence

The recommendations around refocusing our intelligence effort are viewed by the Task force as a shifting of priorities and reallocation of a portion of our counterterrorism capabilities toward the advanced cyber threat and therefore not expected to drive significant cost growth.

11.1.2 Recommendation: Build/Maintain World-Class Cyber Offense

While the United States needs to scale up its cyber offensive capabilities, the size of force to support cyber offense is not expected to be as large-scale as that to defend its systems. The development of modeling and test capabilities are very important to understand this new domain. The overall investment is expected to be moderate.

11.1.3 Recommendation: Enhance Cyber Defenses

The Department already spends significant resources attempting to defend our networks and protect our data. The enterprise architecture recommendation, coupled with the automation recommendations, should actually reduce some of the effort DoD spends today. Gains in efficiency by eliminating many of the mundane tasks through automation can be used to expand Department's efforts toward hunting for intruders within DoD's networks. The Task Force expects the overall cost to remain about the same as today, but the performance results and efficiencies should improve dramatically.

11.1.4 Recommendation: Change DoD Cyber Culture

While a huge challenge for the Department, money is not a limiting factor. The price to execute this recommendation is measured in the will and determination of DoD leadership. Training expense, which is a time cost only for people already paid for through department budgets, is not expected to impact budgets.

11.1.5 Recommendation: Incorporate of Cyber Requirements into System Lifecycle

The Task Force focused on the expense of introducing cyber requirements to acquisition programs. If done carefully, rolling cyber requirements into new programs throughout the lifecycle should drive only moderate costs into those programs. The alternative is to continue building systems that have little chance of performing as expected in the face of a peer adversary. Developing and gaining experience in building testable cyber requirements will take

time and require developing the workforce to manage through the Department. The DoD must avoid the trap of trying to require a system to be defendable against all comers, thereby putting an ever-evolving (and un-testable) requirement onto the acquisition community and the development contractor(s). The focus must be on architectures and techniques that allow the systems to be adapted as cyber threats evolve, and can be tested along the way. (We can test an alternate communications path, a degraded operations mode, overflow buffers in a processor, etc.)

The Task Force recommends beta testing new requirements on the defined critical systems first, then using that experience to impact ACAT 1 programs, and continuing to smaller efforts.

12.0 Summary of Study Recommendations

12.1 Recommendation: Protect the Nuclear Strike as a Deterrent (for existing nuclear armed states and existential cyber attack).

- SECDEF assign USSTRATCOM the task to ensure the availability of Nuclear C3 and the Triad delivery platforms in the face of a full-spectrum Tier VI attack – including cyber (supply chain, insiders, communications, etc.)

This Task Force recommends immediate action to assess and assure to national leadership that the current U.S. nuclear deterrent is also survivable against the full-spectrum cyber Tier V-VI threat described in the taxonomy of this report. Note that a survivable nuclear triad within a full-spectrum, cyber-stressed environment is required regardless of whether or not one believes U.S. *retaliatory response with our nuclear forces* is a credible response *to a major cyber attack.* In other words, the basic characteristics of the traditional U.S. nuclear deterrent incorporates survivability as a basic precept; now the U.S. must add survivability in the event of a catastrophic cyber attack on the country as a basic precept.

12.2 Recommendation: Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary.

- SECDEF and CJCS (12 months)

The Task Force is confident in the need for assured operation to all three – cyber, protected-conventional, and nuclear – capabilities, including their required C3I infrastructures, against advanced cyber threats. Further analysis is necessary to determine the optimal mix of these capabilities, especially the role of offensive cyber and protected-conventional to form the rungs of an escalation ladder designed to introduce elements of deterrence against V-VI attackers.

As a starting point, the Task Force proposes the basic force elements comprising a protected-conventional capability take the form of a survivable second strike conventional mission listed below:

- Long-Range Bombers with precision cruise missiles – currently operational with varying force mix options and numbers
- SSGN with long-range precision cruise missiles – currently operational with capability up through Tomahawk Block IV (offering an upper limit of greater than 600 weapons assuming four SSGNs at sea)
- Conventional ballistic missiles or ballistic/glide hybrids--none currently operational; experimental concepts being tested.
- Survivable national and CCMD C2 leveraging nuclear thin line
  - Build “true” Out-of-Band Command and Control for the most sensitive systems

- War reserve simplified operating systems

12.2.1.1 SECDEF assign UCP Mission of Protected -Conventional Strike to USSTRATCOM.

- USSTRATCOM given target for IOC (24 months)
- USSTRATCOM provide desired planning factors (pre-"launch" survivability, Communications and C2 reliability, targeting/damage expectancy, etc) (6 months)
- USD(AT&L), in coordination with CIO, perform an SoS analysis on selected conventional strike capabilities to determine risk and define an acquisition plan to ensure an enduring survivable capability (6 months)

12.2.1.2 DoD engage multi-agency counterparts for an updated Strategic Deterrence Strategy in 2014 NPR – cyber escalation scenarios on both sides (12 months)

12.3 Recommendation: Refocus Intelligence Collection and Analysis to Understand Adversarial Cyber Capabilities, Plans and Intentions, and to Enable Counterstrategies.

- SECDEF, in coordination with the Directors of CIA, FBI, and DHS, should require the DNI to enhance intelligence collection and analysis on high-end cyber threats. Request the creation of an intelligence community-wide implementation plan that defines implementable enhancements, and their resource impact on DoD and DHS elements, and CIA and FBI. (12 months)

Subversions of sophisticated hardware and software system are extraordinarily difficult to detect through testing and inspection. This led the DSB Task Force to conclude that deeper intelligence about adversaries' offensive software and hardware tools is essential to counter high-end, state-sponsored cyber threats, because it can help focus U.S. efforts on likely targets of compromise.

This intelligence must include:

- Identification and understanding of adversarial cyber weapon development organizations, tools, leadership, and intentions;
- Development of targeting information to support initiatives to counter cyber weaponization;
- Accurate assessment of adversarial plans and capabilities for policy makers.

12.3.1 In response to state-sponsored threats, the Task Force recommends the creation of a counterintelligence capability to directly address the most sophisticated threats using tools and techniques derived from both defensive and offensive U.S. cyber programs.

- Additional details are provided in Appendix 6.

12.4 Recommendation: Build and Maintain World-Class Cyber Offensive Capabilities (with appropriate authorities).

12.4.1 Commander USCYBERCOM Develop a Capability to Model, War Game, Red Team and Eventually Train for Full Scale Peer-on-Peer Cyber Warfare.

- Select an FFRDC-like Center of Excellence. (within 6 months)
- Develop capability to model peer-on-peer (red & blue with supporting situation awareness tools and techniques) full-scale conflict, similar to nuclear exchange models (trigger uncertainties, deliver link probabilities, blow-back risk, recovery abilities and timelines, etc.) (IOC within 18 months of contract award)
- Develop model and validate—evolve through red team and cyber range/war game exercises. Move beyond tabletop level of sophistication. (IOC within 18 months of modeling capability)

Planning for and successfully executing a single offensive cyber operation requires a significant broad set of competencies (e.g. computer science, engineering, encryption, linguistics, geo-political context, military planning and targeting, and more). Given peer and near-peer adversaries who may wish to challenge the United States via cyber aggression, the DoD must develop the capacity to conduct many (potentially hundreds or more) simultaneous, synchronized offensive cyber operations, while defending against a like number of cyber attacks. Understanding interactions and dependencies involved in large scale cyber battle will be required to plan the battle, determine the scale of forces required, and conduct operations at time of conflict.

Moreover, the adversary gets a vote. Cyber war is unlikely to be fought as the United States might like to assume it will be. The United States must be ready to adapt to an adversary that is willing to create its own rules.

12.4.2 USD(P) should establish a policy framework for Offensive Cyber Actions to include who has what authority (for specific actions), under what circumstances, under what controls.

- Completion Date: 18 Months

The appropriate authorities must exist with those responsible to protect U.S. interests. Cyber actions can take place in very short time periods and those responsible to protect the country must understand their roles and authorities. This Task Force has not extensively studied or made recommendations about the definition of "appropriate authorities." Several other efforts are underway in the administration to address this issue and DoD is only one of many players in the broad protection of the United States against cyber attack.

12.4.3 Commander, USCYBERCOM to increase the number of qualified cyber warriors, and enlarge the cyber infrastructure commensurate with the size of the threat.

- Completion Date: 18 Months

The DoD has qualified cyber warriors today, who are supported by robust training programs and cyber toolsets. However there appears to be a "burnout factor" beginning exhibit itself among these elite people. The Department must scale up efforts to recruit, provide facilities and training, and use effectively these critical people.

12.4.4 USD(P&R), in collaboration with the Commander, USCYBERCOM and the Service Chiefs establish a formal career path for DoD civilian and military personnel engaged in "Offensive Cyber Actions"

- Address training and certification requirements
- Define career designations
- Define incentives for personnel achieving higher levels of certification
- Ensure that there is a cadre of high-end practitioners
- Completion: 18 Months with quarterly reviews with the DEPSECDEF

"Cyber Warrior" is a new domain for the Department, and this new class of job will require career paths, training expectations and incentives to attract and develop the needed expertise. It is not clear that high-end cyber practitioners can be found in sufficient numbers within typical recruitment pools. The DoD has the ability to define what it needs and adjust its personnel policies to enable achievement of that goal.

12.5 Recommendation: Enhance Defenses to Protect Against Low and Mid-Tier Threats.

12.5.1 Recommendation: Establish an enterprise security architecture, including appropriate "Building Codes and Standards", that ensure the availability of enabling enterprise missions. The architecture should allow for the ability to:

- Segment the network
- Provide continuous monitoring and situational awareness
- Automate patch and threat management functions
- Audit to the enterprise standard
- Recover to a known (trusted) state
- Provide out-of-band command and control for most sensitive systems

- Responsibility: DoD CIO (in collaboration with Military Departments and Agencies). Due Date – 6 months

The goal of a consistently applied and managed architecture across the Department is to take the low-tier threats off the table, thereby reducing the noise level on DoD networks. More effective mitigation of mid and high tier threats then becomes feasible.

12.5.1.1 Segment the Network

The Department already operates a mesh of networks that can be controlled independently. That concept should be extended through all operational war fighting systems, and tests/trials/red teams should be conducted to understand the capabilities and impacts of disconnecting an infected network to prevent infection of other, interconnected networks.

12.5.1.2 Provide Continuous Monitoring and Situational Awareness

Sensor deployment has begun at Internet access points to monitor and control access and network traffic flow. Commercial tools have advanced to include capabilities to operate behind firewalls and to track anomalous activity throughout the components of a network. It is essential to provide continuous monitoring of all networks against cyber attack (see State Department example in Figure 8.1).

The information assurance of operational systems is typically achieved through encryption of data during network transport (and occasionally at rest - while stored) or multi-level security solutions geared toward the safe handling of multiple security levels of data on the same computer (processor). Data must be decrypted prior to processing, and advanced attacks being used today access the data at that point, thereby circumventing the encryption.

Little consideration goes into military system design today on providing test points that can report system health and operation (sensors). Are checksums overflowing in the processor? Is the processor conducting unexpected computations? There are many “tells” (symptoms) that could be detected and reported. And although such test points and their data transmission would also become targets for cyber attack, an adversary must now have a more detailed understanding of system internals to design a successful attack.

12.5.1.3 Automate Patch and Threat Management Functions

The scale of manual efforts is largely driven by legacy systems using unsupported software operating systems and the lack of consistency in network technology implementation across the Department. The recommendation to isolate systems utilizing older software (no longer maintained by commercial industry) means those systems are removed from the group of components that is regularly updated for malware and other software attacks and then assuming that those systems are likely compromised. The larger GIG is then protected from those systems through strong interface firewalls and detection software.

Most of the COTS technologies available today have user interfaces that allow high levels of flexibility for determining what is deemed unusual network behavior, allowing system administrators to adjust and adapt the monitoring systems as threats evolve.

12.5.1.4 Audit to the Enterprise Standard

Conduct audits and in-process reviews to develop migration and mitigation strategies (systems that cannot be maintained in a timely matter should be restructured into enclaves and isolated from the GIG through firewalls).

The most important part of the recommendation concerns accountability and consistency that must come from senior leadership support and enforcement. Without this management imperative, an attempt at cultural change to improve cyber security will not be taken seriously within the Department.

12.5.1.5 Build Network Recovery Capability

It is not unusual for a sophisticated adversary, who has infiltrated a network, to monitor in real time as the network owners try to kick them out. Frequently, the adversary then implements a counter to the network owner's defensive actions and can be back in the network in a matter of minutes or hours. To fight and win in a war that includes cyber capabilities, DoD can't afford to have the enemy inside its control loops. If DoD is in that situation, then it needs backup (war reserve) mechanisms for C2. Less critical systems need the ability to communicate over an alternative system to address network intrusions, forcing an adversary to penetrate multiple systems and be able to operate both in an integrated, real time fashion to track DoD counterattacks.

12.5.1.6 Recover to a Known (Trusted) State

The goal DoD for operational systems should be to:

- Develop the ability to know (and report) if the network or system has been penetrated,
- Gracefully degrade or have provision for alternate mechanisms to continue the most critical mission functions and
- Recover eventually to a known (trusted) state.

Earlier recommendations addressed the first two goals. The last goal is perhaps the most challenging.

The Department must develop methods to evolve trusted copies of operating software for systems that ensure only the desired changes are made in the "gold copy". The Department should continue to search the commercial and contractor space to develop tools with higher levels of automation for this function.

12.5.2 Recommendation: The DoD should leverage commercial technologies to automate portions of network maintenance and "real-time" mitigation of detected malware.

- Build on existing tools and capabilities currently in use
- Automate response to threat conditions
- Leverage cyber ranges to test emerging technology and develop TTPs and guide investment strategies
- Develop mitigation/transition plans for legacy systems

- Responsibility: DoD CIO, with support from NSA-IAD, IOC: 6 months, with enhancements released on a quarterly basis

As discussed above, modern COTS software has dramatically improved and can provide automation of several key network management functions. The software products sit at the firewall and behind the firewall, which is particularly important to find and track advanced persistent threats.

While these technologies do not address Tier V-VI threats directly, when properly deployed, they make an attacker's task of moving data throughout the systems, while remaining undetected, much more difficult. Our goal is to raise the costs for the Tier V-VI attackers to succeed, limiting the number of operations they can afford to attempt.

12.5.3 Recommendation: USD(P&R) should, in collaboration with the DoD CIO and the Service Chiefs, establish a formal career path for DoD civilian and military personnel engaged in cyber defense

- Address training and certification requirements
- Define career designations
- Define incentives for personnel achieving higher levels of certification
- Ensure that there is a cadre of high-end practitioners
- Completion: 18 Months with quarterly reviews with the DEPSECDEF

The Task Force expects cyber-focused personnel to move between offensive and defensive focused posts throughout their career. The best defenders will be those who understand what can be accomplished from an offensive point of view (the reverse is also true). Creating cyber warriors with expertise in offensive and defensive cyber skills should be encouraged.

12.6 Recommendation: Change DoD's Culture Regarding Cyber and Cyber Security.

12.6.1 Establish a DoD-wide policy, communication, and education program to change the culture regarding cyber and cyber security

SECDEF, CJCS and their direct reports should communicate a vision of DoD Cyber Security for 2020. The Secretary and Chairman should provide direct communication to all organizational

elements explaining the threat and consequences of cyber actions is essential to change DoD's cyber culture. Leadership must change the current culture which is focused on an overwhelming emphasis on operational objectives and shaped by daily exposure in civil cyberspace that imposes little cost to risky behavior.

- Commander, USCYBERCOM and the DoD CIO should establish a plan with measureable milestones and flow-down to all organization elements. The plan must comprise:
  - The policy, operational rules, and expectations for secure use of DoD networks and systems
  - The training program and follow on continual reinforcement of the policy
  - A small "tiger team" of experts to monitor, test, and catch breaches in policy
  - Clear punitive consequences for breaches of policy

- Following the education period and a short grace period, penalties should be imposed similar to the breach of policy for classified material.

- Command readiness should assess and report cyber policy compliance. SECDEF should require the policy to be communicated within 60 days and the education and roll out to every DoD and contractor employee within 9 months.

The current DoD Directive (DoDD 7730.65, dated April 23, 2007) must be modified to include readiness criteria for cyber capability. Specific performance measures related to the IT components critical to the successful execution of the mission must be used to assess Commanders on unit fitness to execute assigned missions and the readiness system must incorporate penalties for failure to meet specific standards.

12.7 Recommendation: Build a Cyber Resilient Force.

12.7.1 DEPSECDEF should direct specific actions to introduce cyber resiliency requirements throughout DoD force structure.

12.7.1.1 The DoD CIO, in coordination with USD(AT&L) should establish a resiliency standard which can be used to design, build and measure capability against. The Joint Staff will use the standard to inform the requirements process.

Realizing that the standards are likely to evolve as the cyber threat evolves, the Task Force identified certain characteristics that the Department should address as it develops the standards and requirements for cyber resiliency to apply to key conventional force capabilities designated as components of the escalation ladder described in Chapter Five. These include:

- Until a return to a TRUSTED, known state capability is developed, the forces and capability components providing a cyber-critical, survivable mission must be controlled throughout their lifecycle and segregated from general purpose forces, including use of and connection to general force networks. Segregation must provide sufficient capability to provide a credible component of the escalation ladder, yet not be so large as to create a resource black hole.
- Maintaining component awareness/control is an important feature of resiliency. Desired awareness measures include sensing and reporting of buffer overflow conditions and bit parity checks, reporting and control of update/file transfer points (e.g. USB ports), and in the future-- real time or near real time monitoring at the component level to ensure authentic components/software are installed.
- Maintain network awareness/control. Install sensing points to measure network performance and patterns, develop and maintain trusted log audit capability, and incorporate trusted and automated patch/update capabilities.
- Support the operational environment such as the conditions under which a system can be connected to specified network, conditions under which it must be disconnected or operate in a degraded mode (e.g. using an out-of-band path that supplies x% of the unfettered capability), and recovery mechanisms.

The Department must write achievable and testable requirements. For example, establishing a requirement that "System X" must be protected against a Tier III-IV threat will force the test community to engage in an infeasible activity as they are forced to certify a system against undiscovered vulnerabilities. The Task Force is wary of the efficacy of establishing a resilience "ility" to work in the same trade space as other "ilities". This approach tends to be bureaucratic and prior to adoption, must demonstrate effectiveness against the cyber threat.

12.7.1.2 Apply the cyber resiliency standard to the segmented force identified as part of the escalation ladder described in Chapter Five.

In the absence of a cyber threat the segmented forces are likely to possess slightly less capability than their non-segmented counterparts due to the isolation from every part of the supporting infrastructure which generates so much advantage to DoD. However, in the face of an adversary employing cyber, the segmented forces will provide far more capability than their non-segmented counterparts.

Subsets of the cyber resiliency requirements for cyber critical survivable missions should be incorporated into the rest of the force structure to defend against Tiers I/II, mitigate the effects of Tier III-IV attacks, and drive up the costs for Tier V-VI attacks.

12.7.1.3 Feedback from testing, red teaming, intelligence community, and modeling and simulation should be increased as a development mechanism to build out DoD's cyber resilient force (USD(AT&L), USD(I), DOT&E, SAEs, CJCS).

DoD must ensure feedback from these exercises impacts system designs, upgrades, CONOPs and TTPs. Lacking a full-scale cyber conflict, DoD will struggle to understand the full implications and effects of the cyber threat. DoD must fight through compartmentalization, understand a nascent but significant capability with limited real operational experience, and avoid typical first adopter mistakes to maximize its resiliency while retaining the huge advantage gained through the networking. The feedback mechanism will also aid the creation of processes to inform development efforts for new and evolved cyber threat vectors.

12.7.1.4 For programs not part of the segmented force, a cyber standard set of requirements (expected to be a subset of the critical program requirements list) should be applied to all DoD programs (USD(AT&L), DoD CIO, SAEs)).

The DoD CIO, in coordination with USD(AT&L) should establish a subset of the resiliency standard developed above which can be applied to the rest of the force structure. The subset should be applied at every available opportunity (e.g. new starts, refurbishment, and repair). Legacy systems unable to meet the standard should be isolated or replaced.

The Department must still discipline itself in its application of the subset of resiliency standard to the rest of the non-escalation ladder components. Not every capability must protect against a Tier III-IV threat but all must defend against a Tier I-II threat. In addition, initial incorporation of the subset of the resiliency standard is likely to require dedicated management to identify and overcome the issues with implementation. The Task Force urges the Department to apply the initial subset of resiliency standards to ACAT 1 programs. Once experience is gained, the resiliency standard can be applied across the Department.

Lacking a full-scale cyber conflict, DoD will struggle to understand the full implications and effects of the cyber threat. The feedback mechanism will also aid the creation of processes to inform development efforts for new and evolved cyber threat vectors.

12.7.1.5 A DoD--wide cyber technical workforce should be developed to support the build-out of the cyber critical survivable mission capability; it should then be rolled out to DoD force structure (USD(AT&L), CIO, SAEs, DOT&E, USD(I) and USD(P&R)).

The technical cyber workforce must function across the capability lifecycle. Similar to the requirements to develop and attract the correct level of cyber talent for DoD's offensive and defensive missions, USD(P&R) must develop supporting policies to build the cyber workforce. The Acquisition Community (e.g. Development Centers, Depots and industrial partners) bears a significant responsibility in this endeavor

along with the operational forces, test community, and scientific and engineering community.

12.7.1.6 The Science and Technology community should establish a secure system design project with Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), academia, commercial and defense industry (ASD R&E)).

Areas to be pursued in the longer term should include: development of special purpose system architectures with inherent resilience, systematic analysis of potential modes of cyber vulnerability of systems, use of emerging technology developments for system resilience (such as trust anchors), minimal functionality components, simplified operating systems, developing a means to verify compromise of fielded systems contributing to critical missions, creating trust in systems built with un-trusted components, and restoring to a known state ("gold standard").

12.7.1.7 The Intelligence Community should initiate a supply chain collection activity (USD(I)).

The DoD should assess the end-to-end process by which electronic "parts" and systems are produced by select companies to determine if what is known of the Cyber threat vectors, including those in Tier V-VI, is appropriately reflected in the efforts of the suppliers.

The DoD must similarly assess the software supply chain to gain an understanding of the cyber threat vectors and to understand where mitigation might be possible, practical and affordable.

The Intelligence Community must be tasked with specific collection, analysis and reporting requirements on the cyber threat vectors, priorities and activities of U.S. adversaries. Although DIA has initiated efforts to provide supplier threat information to the MDAP acquisition community, it is not sufficiently broad or mature to serve the needs of critical mission systems. Mechanisms must be developed to share the resulting intelligence assessments, as appropriate, among the significant players in the DoD supply chain and broader national industries.

Appendix 1—Terms of Reference

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAY 19 2011

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board (DSB) Task Force on Resilient Military Systems

You are hereby directed to establish a Task Force to assess issues affecting the resiliency of military systems that rely on information and communication technology (ICT), including through consideration of the following for mission operational systems:

- Identify measures and techniques under development in the ICT space to quantify system vulnerability and the effectiveness of defense measures;
- Dissect the concept of operations (CONOPS) of various potential cyber attacks and describe the opportunities in the system to develop diagnostics relating to detecting and understanding the attack;
- Apply the diagnostics to 2-3 different mission threads to understand the differences in risk among different types of architecture components (e.g., hardware, software, network, and human risks);
- Study tool/modeling opportunities to predict/measure system vulnerabilities.
- Assess techniques/processes to identify the applicability of human suitability and reliability (e.g., the Personnel Reliability Program);
- Define meaningful measures and metrics to evaluate and monitor the level of system resiliency. Survey metrics developed to characterize resilience in other domains (e.g., insurance, financial systems, and security systems); and
- Identify tactics, procedures and design techniques that could improve system resiliency. In addition, identify research opportunities and estimate the level of investment to achieve results consistent with DoD needs.

Innovative use of modern ICT (e.g., networks, software and microelectronics) in military systems plays a key and vital role in making the U.S. military second to none. However, the effectiveness of these military systems is extremely dependent upon the information assurance provided by its ICT underpinnings and on the personnel who operate and maintain the systems. An unintended consequence of the reliance on ICT to sustain superior U.S. capability is that our adversaries can erode or eliminate our advantage by targeting and exploitation at both the system and component level.

Several factors complicate the ability to maintain our advantage. A short, but certainly not comprehensive, list would identify the complex technology involved, the slowness to understand the problem, and the difficulty to develop effective metrics.

OSD 04475-11

Based in part on the complexity of modern software and microelectronic systems, very small and difficult-to-detect defects or subversive modifications introduced at some point in the life cycle of the systems create debilitating effects. As an example, although remote software system upgrades (remote provisioning) provide great flexibility and efficiency, they also introduce a very attractive vector for an enemy to compromise a system. The same complexity amplifies the human factor – whether malicious or innocent. Insertion of an infected flash drive produced the most significant breach of U.S. systems to date; while the intentional downloading of thousands of classified documents to "music"-labeled CDs generated its own set of problems. As a result of the great and growing complexity of DoD systems, cyber resiliency is an extremely broad and difficult attribute to guarantee.

DoD and military officials have long understood our advantage in the utilization of these technologies in military systems. Unfortunately, DoD officials have been slow to develop sufficient understanding of the mission assurance implications of adversary capability to operationally exploit these systems. Although the contest is simple to characterize, it is an extremely complex matter and a difficult one in which to achieve confidence in the desired outcome. To continue to take advantage of modern technology to increase our military effectiveness, we must possess sufficient confidence that these systems are not compromised to such a degree that we lose the benefit. In addition, we want to work actively to decrease the confidence of our adversaries that their clandestine operations targeting our systems are effective enough to eliminate our advantage.

An important step toward designing, implementing, and maintaining more resilient systems is to understand how to measure the resiliency of those systems relative to various cyber attacks and adversaries. Establishing useful measures and metrics is a first step toward quantifying and developing systematic methods and standards to improve both real resiliency and confidence in our process. These tools would allow organizations to apply scarce resources (people and dollars) more effectively in all phases (research, acquisition, and maintenance) of the life cycle of these systems to improve our confidence in the resiliency of these capabilities, and to enhance the ability of those systems to perform as expected in a hostile environment.

Prior efforts to develop useful measures and metrics have largely failed due to the difficulty of the subject. There is no guarantee that this effort will fare better. However, if fully adequate and robust metrics are not developed, the Task Force will describe the weaknesses of the proposed metrics and describe an iterative process to obtain improved metrics over time.

Administration support and funding will be provided by the Under Secretary of Defense for Acquisition, Technology, and Logistics. Additional support will be provided by the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, the Director, Operational Test and Evaluation (DOT&E), the Vice Chairman of the Joint Chiefs of Staff, and the Commander, U.S. Cyber Command. All Task Force members, consultants, and supporting personnel will be appointed or designated in accordance with DoD Instruction (DoDI) 5105.04, "Department of Defense Federal Advisory Committee Management Program."

The Task Force will be established and operated in accordance with the provisions of the "Federal Advisory Committee Act" (5 U.S. Code Appendix, as amended), DoDI 5105.04, the DSB Charter, and all applicable laws, policies, and regulations. It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of section 208 of title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.

Appendix 2—Task Force Membership

Co-Chairs

Mr. James R. Gosler	Sandia National Laboratory
Mr. Lewis Von Thaer	General Dynamics

Executive Secretary

Mrs. Kristen Baldwin	OASD(R&E)
Mr. Steve Gates	ODT&E

Members

Dr. Allen Adler	The Boeing Company
Dr. James Babcock	Northrop Grumman
Mr. Dean Clubb	Independent Consultant
Dr. Craig Cook	MITRE
Dr. Donald Duncan	Johns Hopkins University/APL
ADM William J. Fallon, USN (Ret.)	Independent Consultant
Mr. Robert Gourley	Crucial Point, LLC
Dr. Richard Ivanetich	Institute for Defense Analyses
Dr. Ronald L. Kerber	Independent Consultant
Hon. Donald M. Kerr, PhD.	Independent Consultant
Dr. William LaPlante	MITRE
Hon. Judith A. Miller, Esq.	Independent Consultant
Mr. Al Munson	Potomac Institute for Policy Studies
Mr. Richard Schaeffer	Independent Consultant
Dr. Fred B. Schneider	Cornell University
ADM William Studeman, USN (Ret.)	Independent Consultant
Mr. Michael Swetnam	Potomac Institute for Policy Studies
Dr. Peter Weinberger	Google, Inc.
Dr. Robert Wisnieff	IBM

Government Advisors

Mr. Rick Wilson	National Security Agency
Mr. Mitchell Komaroff	CIO-ODA SD (I&IA)
Mr. RC Porter	Defense Intelligence Agency

Senior Advisors

Dr. Craig Fields	Independent Consultant
Dr. Robert Hermann	Independent Consultant
Mr. Robert Stein	Independent Consultant

DSB Secretariat

Mr. Brian Hughes	Defense Science Board

Lt. Col. Michael Warner, USAF	Defense Science Board
CDR Doug Reinbold, USN	Defense Science Board

Support

Mr. Chris Grisafe	SAIC
Ms. Tammy-jean Beatty	SAIC

Appendix 3—Task Force Meeting Schedule and Briefings

March 16-17 2011		
Title	**Briefer**	**Organization**
AT&T Operations Center Metrics	Mr. Ed Amoroso	AT&T
Cross Sector Information Sharing, Analysis & Collaboration Initiative	Mr. Robert Dix	Juniper Networks
Carnegie Mellon Cyber SOC	Mr. Terry Roberts	Carnegie Mellon University
In-Q-Tel Cyber Measures Research	Mr. Dan Geer	In-Q-Tel
State Department Measures	Mr. John Streufert	Department of State
Why This is So Hard?	Mr. Carl Landwehr	National Science Foundation
Cybersecurity in the Digital Cloud Overview	Dr. Eric Evans	DSB Cybersecurity in the Digital Cloud Task Force
System Security Metrics	Dr. Salvatore J. Stolfo	Columbia University
Metrics, Models, and Analysis of Network Security and Survivability	Mr. Kishor Trivedi	Duke University

April 20-21, 2011		
Title	**Briefer**	**Organization**
DoD Strategy for Operation in Cyberspace	Mr. Robert Butler	OSD Policy
The Supply Chain Threat Assessment Center	Mr. Cal Temple	DIA
Building Resilient Network Architectures	Mr. Kevin Bingham	DoD CIO
Examples of Advanced Cyber Threat Assessments	Ms. Yulin Bingle	DIA
Examples of Cyber Metrics in Use by DoD	Mr. David Aland	DOT&E
Examples of DoD Red Teaming	CAPT Forbes MacVane, USN LCDR John Kaltwasser, USN Mr. Scott Brown	NSA
Examples of Navy Red Teaming Impacts on Military Systems	LT Greg Smith	NIOC

May 17-18, 2011

Title	Briefer	Organization
NCIX	Ms. Margie Gilbert	
NIC	Mr. Sean Kanuck	NIC
TRANSCOM	Mr. Steve Stone CAPT Mike Murray	USTRANSCOM
NCIJTF	Mr. Brad Bleier	NCIJTF
Cyber Analytical Framework	Daniel Kaufman	DARPA
Dynamic Quarantine of Worms Cyber Gnome	Dr. Timothy Fraser	DARPA
TRUST, ISIS (Follow Program)	Dr. Carl McCants	DARPA
National Cyber Range	Dr. Jinendra Ranka	DARPA
Cloud to the Edge	Dr. Keith Gremban	DARPA
Vulnerability Assessment: Virtual Machine	Mr. Tony Sager	NSA/CSS
Terremark	Ms. Jamie DosSantos	Terremark, Inc.
Systems Security Engineering	Ms. Jennifer Bayuk	Independent Consultant
Research Roadmap	Mr. Barry Horowitz	University of Virginia
June 23-24, 2011		
Title	**Briefer**	**Organization**
Terminal Fury	Mr. David Aland	DOT&E
DIB Cyber Security	Mr. Steven D. Shirley Mr. Jeffrey Stuzman	DoD Cyber Crime Center
NSA High Assurance Platform	Mr. Neil Kittleson	NSA/CSS
Virtual Secure Enclave	Dr. Matt Goda	USPACOM
NSA Gold Standard	Ms. Carol Walters Mr. Mike Escazage Ms. Ann Erickson Mr. John Schuessler	NSA/CSS
Improving Mission Assurance by Using New Techniques in Network Analysis	Dr. Don Snyder	RAND Corporation
Resilience Metrics	Dr. Erik G. Mettala	Battelle
NRO Information Assurance	Ms. Bonnie Paul	NRO
July 18-19 2011		
Title	**Briefer**	**Organization**
Neural IQ	Mr. Bill Stacia	Neural IQ
Measuring Cyber Vulnerabilities and Response Effectiveness	Mr. Mike Papay	Northrop Grumman
Measuring Security	Mr. Steve Lipner	Microsoft
Security and Resiliency	Mr. Michael Berman	Catbird
Cyber Resilience	Mr. Iven Connary	Q1 Labs
August 10-11, 2011 (Joint Meeting with Cloud TF, 8/11)		
Title	**Briefer**	**Organization**

DoD CIO Briefing	Ms. Teri Takai	DoD CIO
Cyber Law and Policy	Dr. Catherine Lotrionte	Georgetown University Law Center
Bromium	Mr. Simon Crosby	Bromium Inc.
Cloud Computing: Key Questions	Ms. Melissa Hathaway Mr. G. Gaffney	Hathaway Global Strategies DNI
September 22-23, 2011		
Title	**Briefer**	**Organization**
IDA Brief	Dr. Margaret Myers	Institute for Defense Analyses
United States Cyber Command	Mr. Mark Young	USCYBERCOM
October 24-27, 2011 (Offsite Joint Meeting with Cloud TF, 10/27)		
Title	**Briefer**	**Organization**
United States Cyber Command	Mr. Mark Young	USCYBERCOM
November 17-18, 2011		
Title	**Briefer**	**Organization**
DDR&E Resilient Systems Program	Dr. Steve King	DDR&E
DoD CIO and the Working Group on Network Resilience	Ms. Laura Boehm	DoD CIO
Secure Configuration Management	Mr. Kevin Dulany Ms. Robby Ann Carter	DIAP
January 19-20, 2012		
Title	**Briefer**	**Organization**
Law and Policy Discussion	Mr. Gary Sharp	DoD
February 9-10, 2012		
Title	**Briefer**	**Organization**
Cyber Deterrence	Ms. Michelle Markoff	State Department
Conventional Thin Line	Mr. Dave Dick Mr. Carl Prantl	OSD

Appendix 4—Acronyms Used in This Report

ACAT	Acquisition Category
ASD(R&E)	Assistant Secretary of Defense for Research and Engineering
C2	Command and Control
C3	Command, Control, Communications
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAC	Common Access Card
CCC	Cyber Conflict College
CCMD	Combatant Command
CCR	Centers for Communication Research
CEO	Chief Executive Officer
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CJCS	Chairman of the Joint Chiefs of Staff
CNDSP	Computer Network Defense Service Provider
CNE	Computer Network Exploitation
COG	Continuity of Government
CONUS	Continental United States
COTS	Commercial off the Shelf
CPGS	Conventional Prompt Global Strike
CSIA	Cyber Security/Information Assurance
DARPA	Defense Advanced Research Projects Agency
DASD(SE)	Deputy Assistant Secretary of Defense for Systems Engineering
DEPSECDEF	Deputy Secretary of Defense
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIAP	Defense Information Assurance Program
DIB	Defense Industrial Base
DISA	Defense Information Systems Agency
DNI	Director of National Intelligence
DoD	Department of Defense
DOS	Department of State
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities
DSB	Defense Science Board
DSP	Defense Service Provider
EA	Enterprise Architecture
EMP	Electromagnetic Pulse
FBI	Federal Bureau of Investigation
FFRDC	Federally Funded Research and Development Center
GIAP	Global Information Assurance Portfolio
GIG	Global Information Grid
GWOT	Global War on Terror

HBSS	Host Based Security System
HUMINT	Human Intelligence
IA	Information Assurance
IC	Intelligence Community
ICBM	Intercontinental Ballistic Missile
ICIECS	International Conference on Information Engineering and Computer Science
ICT	Information and Communications Technology
IED	Improvised Explosive Device
IOC	Initial Operating Capability
IP	Intellectual Property
IPB	Intelligence Preparation of the Battlespace
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
JPIOE	Joint Intelligence Preparation of the Operational Environment
JROC	Joint Requirements Oversight Council
MDAP	Major Defense Acquisition Program
NC2	Nuclear Command and Control
NDU	National Defense University
NIPRNet	Unclassified but Sensitive Internet Protocol (IP) Router Network
NIST	National Institute of Standards and Technology
NPR	Nuclear Posture Review
NSA	National Security Agency
NSA-IAD	National Security Agency Information Assurance Directorate
ODNI	Office of the Director of National Intelligence
OPLANS	Operational Plans
OSD	Office of the Secretary of Defense
PKI	Public Key Infrastructure
POTUS	President of the United States
PPBS	Planning, Programming and Budgeting System
SAE	Service Acquisition Executives
SCADA	Supervisory Control and Data Acquisition
R&D	Research and Development
SCRM	Supply Chain Risk Management
SCADA	Supervisory Control and Data Acquisition
SECDEF	Secretary of Defense
SIGINT	Signals Intelligence
SIPRNet	Secret Internet Protocol Router Network
SIGINT	Signals Intelligence
SLBM	Submarine-Launched Ballistic Missile
SLOC	Source Lines of Code
SOF	Special Operations Forces
SoS	System of Systems
SSGN	Cruise Missile Submarine
TF	Task Force
TTP	Tactics, Techniques, and Procedures
UARC	University Affiliated Research Center
UCP	Unified Command Plan
USCYBERCOM	United States Cyber Command

USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary for Defense Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USSTRATCOM	United States Strategic Command

Appendix 5—Sample Enterprise Specification

INFORMATION SECURITY HANDBOOK APPENDIX A: ATTACHMENT 1: COMPANY ADDED SECURITY CONTROLS	5/16/2011

AC-8 System Use Notification

AC8 -1 Each notification message shall have legal review at the BU and approval by Legal at Corporate Headquarters prior to implementation.

AC-17 Remote Access

AC17 -1 Internal network level access via VPNs or dial-up will be provided only to Company approved information assets.

AC17-2 SSL VPN/Web VPN: Application level access via a "Secure Socket Layer (SSL) VPN" or "Web VPN" is authorized for users using any internet-connected computer with a web browser. SSL VPN access is restricted to specific BU designated applications.

AC-19 Access Control for Portable and Mobile Devices

AC19-1 Users are required to protect mobile computing devices used to exchange BU or enterprise information based on the local threat level and the local surroundings (e.g., lock in vehicle trunk, do not leave unattended in public areas, do not display sensitive data in areas where public viewing cannot be restricted). Increased vigilance is required for travel to higher threat areas.

AC19-2 BU information assets are prohibited from being transported to or from the countries listed below without prior written permission from the Business Unit (BU) Chief Information Officer (CIO) and Security Director. Once approved, it is the BU's responsibility to provide the approved traveler an IT asset with a fresh image and only the required applications and data to support business needs. Upon return from travel, that IT asset shall never connect to the BU or any Company information Infrastructure nor store, transmit, or process Company information and data. No information may be electronically transferred from the returned asset to any other Company IT asset.

Company employees (and those contractors currently assigned to Company) who will travel to the countries listed below for company or personal business are required to alert the BU Security Director of the intended travel and receive a security briefing prior to the commencement of said travel

This notice applies to the following countries:

- Armenia
- Azerbaijan
- Albania
- Belarus
- Cambodia
- China (People's Republic of China)
- Cuba
- Georgia
- Hong Kong (SAR)
- Iran
- Iraq
- Kazakhstan
- Korea, North
- Kyrgyzstan
- Laos
- Libya
- Macau
- Moldova
- Mongolia
- Russia
- Sudan
- Syria
- Tajikistan
- Turkmenistan
- Taiwan (Republic of China)
- Uzbekistan
- Vietnam

INFORMATION SECURITY HANDBOOK APPENDIX A: ATTACHMENT 1: COMPANY ADDED SECURITY CONTROLS	5/16/2011

AC-20 Use of External Information Systems

AC20-Company-I Connection non-BU equipment to the BU information technology infrastructure requires the prior written authorization of the BU CIO and BU Security Director.

AC20-Company-2 Users shall not store Company data on any personally owned computer or media.

AT -3 Security Training

AT3-Company-1 The BU shall ensure that all employees or contractors who are involved with the architecture or management of the BU's Information Security infrastructure receive appropriate minimum of three security related training modules or courses annually

AU-II Audit Record Retention

AU-II-Company-1 All system generated audit records shall be retained for a minimum of30 days.

CA-3 Information System Connections

CA3-Company-1 The BU shall prohibit the creation of unauthorized networks.

IA-2 User Identification and Authentication

1A2-Company-I All servers are required to have two-factor authentication for all individuals with Administrator level access. In addition, two-factor authentication will be used where advisable based on potential risk, as determined by a risk assessment of the access situation.

IA2-Company-2 The information system employs multifactor authentication for remote system access.

TA-4 Identifier Management

IA4-Company-I Shared IDs require the authorization of the BU CIO and Director of Security. The BU shall maintain documentation of the business requirement necessitating the shared ID, the mitigating controls implemented to reduce the risk, and the authorization.

IA-5 Authenticator Management

IA5-Company-I There are three means of authenticating a user's identity which can be used alone or in combination:

I. Something the individual knows (a secret--e.g., a password, Personal Identification Number (PIN), or cryptographic key). Passwords must be at least 8 characters long and contain at least one each of the following: upper case alpha, lower case alpha, number, and a special character. If legacy applications or operating systems are unable to meet the minimum password standards, use the strongest setting possible in the application and operating system. The BU shall maintain a list of those applications or operating systems not meeting the Policy, along with security controls used to reduce risk. The degree of sensitivity of the applications or operating systems shall be considered in this process. User Password changes shall be enforced at least quarterly with controls to ensure that passwords are not repeated within a year.

II. Something the individual possesses (a security token--e.g., a smart card); and

III. A unique physical identifier (i.e., a biometric which includes such characteristics as a voice pattern, handwriting dynamics, or a fingerprint).

2

INFORMATION SECURITY HANDBOOK APPENDIX A: ATTACHMENT 1: COMPANY ADDED SECURITY CONTROLS	5/16/2011

IR-6 Incident Reporting

IR6-Company-I	The BU shall provide a notification list to the Company Security Operations Center (SOC) of the personnel to notify about information security incidents that may affect the BU.
IR6-Company-2	The BU shall comply with any government directive to report security incidents to any non-Company entity and inform the Corporate CIO and the Corporate Security Director of such actions. These reports may include notifications to various law enforcement agencies or to a national Computer Emergency Response Team (CERT) per Appendix D.

MP-5 Security Categorization

MP5-Company-I	For all mobile computing devices used to exchange SU or enterprise information, hard drives and media containing Company or client sensitive information (e.g., CDs, USB Memory Sticks, System back-up tapes) shall be encrypted with, at a minimum, the required level of encryption specified in Appendix B if they leave a Company facility.

RA-2 Security Categorization

RA2-Company-I	The BU may implement additional security controls, such as those contained in NIST 800-53 that are not included here, to address unique risks associated with critical information and systems based on the results of a risk assessment or as may be required for compliance with contractual obligations.

RA-3 Risk Assessment

RA3-Company-I	The SU shall perform an information security risk assessment for all new mergers or acquisitions within 60 days of the acquisition.
RA3-Company-2	The BU must conduct a thorough assessment of the infrastructure of any part of the BU being divested prior to the conclusion of the divestiture.
RA3-Company-3	The ISRB will conduct a review of the BU being divested prior to the conclusion of the divestiture to ensure that no Company sensitive information is conveyed and the BU will be properly disconnected from the Company Enterprise.

SA7 - User Installed Software

SA7-Company-I	Only BU-authorized computing devices and software products shall be used to process business data.
SA7-Company-2	The BU shall prohibit the use of common hacker tools (e.g., network scanners, sniffers) unless specifically approved by the BU CIO and Security Director.

3

INFORMATION SECURITY HANDBOOK	EFFECTIVE
Appendix A Security Controls Cross-Reference to NIST 800-53 (rev 3)	5/16/2011

Changes to the Baseline - Effective July 1, 2012, roll-out should be based upon BU Risk-Reward Evaluations

Changes to the Baseline - Effective July 1, 2013 (Security Roadmap)

Access to NIST 800-53 Rev(3) dated 5/1/10:
http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

General Descriptions:

1 Replace "Government" with Company Business Unit
2 Replace 'Federal Information Systems' with Company Business Unit Information System
3 CE's are the NIST 800-53 Control Enhancements
4 Company's additional controls above the NIST 800-53 can be located in Attachment 1 of this Appendix

	Family	Company Clarification/Defined Value	Baseline: Existing	Baseline: All by 7/1/2012	Baseline: Roadmap 7/1/2013	Not Base-lined
	Access Control					
AC-1	Access Control Policy and Procedures	BU defined frequency based upon criticality (Review at least Annually)	✓			
AC-2	Account Management	j. Reviewing accounts on a frequency defined by the Business Unit commensurable to Risk Level of the information system.	✓			
AC-2	CE 1					✓
AC-2	CE 2					✓
AC-2	CE 3					✓
AC-2	CE 4					✓
AC-2	CE 5					✓
AC-2	CE 6					✓
AC-2	CE 7					✓
AC-3	Access Enforcement		✓			
AC-3	CE 1		✓			
AC-3	CE 2					✓
AC-3	CE 3					✓
AC-3	CE 4					✓
AC-3	CE 5					✓
AC-3	CE 6					✓
AC-4	Information Flow Enforcement		✓			
AC-4	CE 1					✓
AC-4	CE 2					✓
AC-4	CE 3					✓
AC-4	CE 4					✓
AC-4	CE 5					✓
AC-4	CE 6					✓
AC-4	CE 7					✓
AC-4	CE 8					✓
AC-4	CE 9					✓
AC-4	CE 10					✓
AC-4	CE 11					✓
AC-4	CE 12					✓
AC-4	CE 13					✓
AC-4	CE 14					✓
AC-4	CE 15					✓
AC-4	CE 16					✓
AC-4	CE 17					✓
AC-5	Separation of Duties		✓			
AC-6	Least Privilege		✓			
AC-6	CE 1					✓
AC-6	CE 2	[BU Defined]		✓		
AC-6	CE 3					✓
AC-6	CE 4					✓
AC-6	CE 5					✓
AC-6	CE 6					✓

	Family	Company Clarification/Defined Value	Baseline			
			Existing	All by 7/1/2012	Roadmap 7/1/2013	Not Base-lined
AC-7	Unsuccessful Login Attempts	[a. 5; b. 30 minutes]	✔			
AC-7	CE 1					✔
AC-7	CE 2	(2) five attempts		✔		
AC-8	System Use Notification	Replace 'US Government' with "Company business unit"	✔			
AC-8	CE-AC8-		✔			
AC-9	Previous Logon (Access) Notification	When designing new applications and operating systems which are deemed sensitive or important, this control should be built into the design.		✔		
AC-9	CE 1					✔
AC-9	CE 2					✔
AC-9	CE 3					✔
AC-10	Concurrent Session Control					✔
AC-11	Session Lock	15 minutes	✔			
	CE 1					✔
~~AC-12~~	~~Session Termination (Withdrawn)~~	Withdrawn from NIST 800-53 Rev(3)				
~~AC-13~~	~~Supervision and Review – Access Control~~	Withdrawn from NIST 800-53 Rev(3)				
AC-14	Permitted Actions without Identification		✔			
	CE 1					✔
~~AC-15~~	~~Automated Marking~~	Withdrawn from NIST 800-53 Rev(3)				
AC-16	Security Attributes					✔
AC-16	CE 1					✔
AC-16	CE 2					✔
AC-16	CE 3					✔
AC-16	CE 4					✔
AC-16	CE 5					✔
AC-17	Remote Access		✔			
AC-17	CE 1				✔	
AC-17	CE 2		✔			
AC-17	CE 3		✔			
AC-17	CE 4					✔
AC-17	CE 5					✔
AC-17	CE 6					✔
AC-17	CE 7					✔
AC-17	CE 8					✔
AC-17	CE-AC17-	Found in Attachment 1 of Appendix A	✔			
AC-17	CE-AC17-	Found in Attachment 1 of Appendix A	✔			
AC-18	Wireless Access		✔			
AC-18	CE 1		✔			
AC-18	CE 2					✔
AC-18	CE 3					✔
AC-18	CE 4					✔
AC-18	CE 5					✔
AC-19	Access Control for Mobile Devices	[BU Defined]	✔			
AC-19	CE 1					✔
AC-19	CE 2					✔
AC-19	CE 3					✔
AC-19	CE 4					✔
AC-19	CE-AC19-_ _ _	Found in Attachment 1 of Appendix A	✔			
AC-19	CE-AC19-	Found in Attachment 1 of Appendix A	✔			
AC-20	Use of External Information Systems		✔			
AC-20	CE 1		✔			
AC-20	CE 2			✔		
AC-20	CE AC20-	Found in Attachment 1 of Appendix A	✔			
AC-20	CE AC20-_ _ _	Found in Attachment 1 of Appendix A	✔			
AC-21	User-Based Collaboration and Information Sharing					✔
AC-21	CE 1					✔
AC-22	Publicly Accessible Content	[BU Defined]		✔		
	Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	BU defined frequency based upon criticality (at least Annually)	✔			
AT-2	Security Awareness	Within 30 days of granting access and at least annually afterwards	✔			

	Family	Company Clarification/Defined Value	Baseline			
			Existing	All by 7/1/2012	Roadmap 7/1/2013	Not Base-lined
AT-2	CE 1					✓
AT-3	Security Training	[BU Defined]	✓			
AT-3	CE 1					✓
AT-3	CE 2					✓
AT-3	AT3-GD-1	Found in Attachment 1 of Appendix A	✓			
AT-4	Security Training Records	Requirement 'a' only	✓			
AT-5	Contacts with Security Groups and Associations					✓
	Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	BU defined frequency based upon criticality (at least Annually)	✓			
AU-2	Auditable Events	a. BU defined; d. BU defined	✓			
AU-2	CE 1					✓
AU-2	CE 2					✓
AU-2	CE 3					✓
AU-2	CE 4					✓
AU-3	Content of Audit Records		✓			
AU-3	CE 1					✓
AU-3	CE 2					✓
AU-4	Audit Storage Capacity		✓			
AU-5	Response to Audit Processing Failures	[BU Defined]	✓			
AU-5	CE 1					✓
AU-5	CE 2					✓
AU-5	CE 3					✓
AU-5	CE 4					✓
AU-6	Audit Review, Analysis, and Reporting	[BU Defined]	✓			
AU-6	CE 1					✓
AU-6	CE 2					✓
AU-6	CE 3					✓
AU-6	CE 4					✓
AU-6	CE 5					✓
AU-6	CE 6					✓
AU-6	CE 7					✓
AU-6	~~CE 8~~ Incorporated into SI-4.					✓
AU-6	CE 9					✓
AU-7	Audit Reduction and Report Generation					✓
AU-7	CE 1					✓
AU-8	Time Stamps		✓			
AU-8	CE 1	(1) Daily and the BU shall implement Network Time Protocol (NTP) services whereby at least one root level NTP device synchronizes with a stratum two time source.	✓			
AU-9	Protection of Audit Information		✓			
AU-9	CE 1					✓
AU-9	CE 2					✓
AU-9	CE 3					✓
AU-9	CE 4					✓
AU-10	Non-repudiation					✓
AU-10	CE 1					✓
AU-10	CE 2					✓
AU-10	CE 3					✓
AU-10	CE 4					✓
AU-10	CE 5					✓
AU-11	Audit Record Retention	In accordance with CP 03-102 and local Records Management polices	✓			
	CE AU-11	Found in Appendix A, attachment 1	✓			
AU-12	Audit Generation		✓			
AU-12	CE 1					✓
AU-12	CE 2					✓
AU-13	Monitoring for Information Disclosure					✓
AU-14	Session Audit					✓
AU-14	CE 1					✓

	Family	Company Clarification/Defined Value	Baseline			
			Existing	All by 7/1/2012	Roadmap 7/1/2013	Not Base-lined
	Security Assessment and Authorization	**The intent behind adding the CA Control family into the GD Baseline control set is not a matter of meeting the requirements of rigorous DOD Accreditation process, but a matter of best practices, that will build the foundation supporting your risk based approach going forward. Included but not limited would be the Security Assessment procedure, the roles of the Business, IT and Security owners, and the Risk Management Strategy.**				
CA-1	Security Assessment and Authorization Policies and Procedures	BU defined frequency based upon criticality (at least Annually)		✓		
CA-2	Security Assessments			✓		
CA-2	CE 1			✓		
CA-2	CE 2			✓		
CA-3	Information System Connections			✓		
CA-3	CE 1			✓		
CA-3	CE 2			✓		
CA-3	CE CA-3	Found in Attachment 1 of Appendix A	✓			
~~CA-4~~	~~Security Certification (Withdrawn~~	Withdrawn from NIST 800-53 Rev(3)				✓
CA-5	Plan of Action and Milestones		✓			
CA-5	CE 1					✓
CA-6	Security Authorization			✓		
CA-7	Continuous Monitoring	Audits, SOC and ISO reviews satisfy this control		✓		
CA-7	CE 1					✓
CA-7	CE 2					✓
	Configuration Management					
CM-1	Configuration Management Policy and Procedures	BU defined frequency based upon criticality (at least Annually)	✓			
CM-2	Baseline Configuration	Security architecture, server, workstation and all critical applications	✓			
CM-2	CE 1			✓		
CM-2	CE 2					✓
CM-2	CE 3			✓		
CM-2	CE 4					✓
CM-2	CE 5					✓
CM-2	CE 6					✓
CM-3	Configuration Change Control	[BU Defined]	✓			
CM-3	CE 1					✓
CM-3	CE 2					✓
CM-3	CE 3					✓
CM-3	CE 4	[BU Defined]		✓		
CM-4	Security Impact Analysis			✓		
CM-4	CE 1					✓
CM-4	CE 2					✓
CM-5	Access Restrictions for Change		✓			
CM-5	CE 1		✓			
CM-5	CE 2					✓
CM-5	CE 3					✓
CM-5	CE 4					✓
CM-5	CE 5					✓
CM-5	CE 6					✓
CM-5	CE 7					✓
CM-6	Configuration Settings	[BU Defined, factoring in Appendix B]	✓			
CM-6	CE 1					✓
CM-6	CE 2					✓
CM-6	CE 3					✓
CM-6	CE 4					✓
CM-7	Least Functionality	[BU Defined, factoring in Appendix B]		✓		
CM-7	CE 1				✓	
CM-7	CE 2					✓
CM-7	CE 3					✓
CM-8	Information System Component	[BU Defined]	✓			
CM-8	CE 1		✓			
CM-8	CE 2					✓

	Family	Company Clarification/Defined Value	Baseline			
			Existing	All by 7/1/2012	Roadmap 7/1/2013	Not Base-lined
CM-8	CE 3					✓
CM-8	CE 4					✓
CM-8	CE 5					✓
CM-8	CE 6					✓
CM-9	Configuration Management Plan				✓	
CM-9	CE 1				✓	
	Contingency Planning	**Each BU shall establish and maintain a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) to ensure that vital business operations continue, regardless of the circumstances.**				
CP-1	Contingency Planning Policy and Procedures	BU defined frequency based upon criticality (at least Annually)	✓			
CP-2	Contingency Plan	b. BU defined; d. Contingency Plan review at least Annually	✓			
CP-2	CE 1		✓			
CP-2	CE 2		✓			
CP-2	CE 3			✓		
CP-2	CE 4					✓
CP-2	CE 5					✓
CP-2	CE 6					✓
CP-3	Contingency Training	At least Annually		✓		
CP-3	CE 1					✓
CP-3	CE 2					✓
CP-4	Contingency Plan Testing and Exercises	BU defines the method(s) and frequency based upon criticality	✓			
CP-4	CE 1		✓			
CP-4	CE 2					✓
CP-4	CE 3					✓
CP-4	CE 4					✓
~~CP-5~~	~~Contingency Plan Update (Withdrawn)~~	Withdrawn from NIST 800-53 Rev(3)				
CP-6	Alternate Storage Site		✓			
CP-6	CE 1					✓
CP-6	CE 2					✓
CP-6	CE 3					✓
CP-7	Alternate Processing Site					✓
CP-7	CE 1					✓
CP-7	CE 2					✓
CP-7	CE 3					✓
CP-7	CE 4					✓
CP-7	CE 5					✓
CP-8	Telecommunications Services					✓
CP-8	CE 1					✓
CP-8	CE 2					✓
CP-8	CE 3					✓
CP-8	CE 4					✓
CP-9	Information System Backup	As needed to support the contingency plan (Control CP-2 Contingency Plan)	✓			
CP-9	CE 1	BU defined frequency based upon criticality (at least Annually)		✓		
CP-9	CE 2					✓
CP-9	CE 3			✓		
CP-9	CE 4					✓
CP-9	CE 5					✓
CP-9	CE 6					✓
CP-10	Information System Recovery and Reconstitution		✓			
CP-10	CE 1					✓
CP-10	CE 2					✓
CP-10	CE 3					✓
CP-10	CE 4					✓
CP-10	CE 5					✓
CP-10	CE 6			✓		

	Family	Company Clarification/Defined Value	Baseline			
			Existing	All by 7/1/2012	Roadmap 7/1/2013	Not Base-lined
	Identification and Authentication					
IA-1	Identification and Authentication Policy and Procedures	BU defined frequency based upon criticality (at least Annually)	✓			
IA-2	Identification and Authentication		✓			
IA-2	CE 1					✓
IA-2	CE 2					✓
IA-2	CE 3					✓
IA-2	CE 4					✓
IA-2	CE 5					✓
IA-2	CE 6					✓
IA-2	CE 7					✓
IA-2	CE 8					✓
IA-2	CE 9					✓
IA-2	IA2-		✓			
IA-2	IA2-		✓			
IA-3	Device Identification and Authentication					✓
IA-3	CE 1					✓
IA-3	CE 2					✓
IA-3	CE 3					✓
IA-4	Identifier Management	d. BU defined e. BU defined inactivity period based upon criticality (not to exceed 180 days)	✓			
IA-4	CE 1					✓
IA-4	CE 2					✓
IA-4	CE 3					✓
IA-4	CE 4					✓
IA-4	CE 5					✓
IA-4	IA4-		✓			
IA-5	Authenticator Management	g. As required	✓			
IA-5	CE 1	(a) At least 8 characters long and contain at least one each of the following: upper case alpha, lower case alpha, number, and a special character. (b) Enforces at least one changed character when new passwords are created; (d) Enforces a 1 day password minimum lifetime and 90 day password maximum lifetime; and (e) Prohibits password reuse for 24 generations.		✓		
IA-5	CE 2					✓
IA-5	CE 3					✓
IA-5	CE 4					✓
IA-5	CE 5					✓
IA-5	CE 6					✓
IA-5	CE 7					✓
IA-5	CE 8					✓
IA-5	IA5-		✓			
IA-6	Authenticator Feedback		✓			
IA-7	Cryptographic Module Authentication				✓	
IA-8	Identification and Authentication			✓		
	Incident Response					
IR-1	Incident Response Policy and Procedures	BU defined frequency based upon criticality (at least Annually)	✓			
IR-2	Incident Response Training	b. At least annually.	✓			
IR-2	CE 1					✓
IR-2	CE 2					✓
IR-3	Incident Response Testing and Exercises					✓
IR-3	CE 1					✓
IR-4	Incident Handling		✓			
IR-4	CE 1	"Automation" is a standard process, a ticketing system, etc.		✓		
IR-4	CE 2					✓
IR-4	CE 3					✓
IR-4	CE 4					✓
IR-4	CE 5					✓
IR-5	Incident Monitoring		✓			
IR-5	CE 1					✓

	Family	Company Clarification/Defined Value	Baseline			
			Existing	All by 7/1/2012	Roadmap 7/1/2013	Not Base-lined
IR-6	Incident Reporting	Refer to Handbook Appendix D	✓			
IR-6	CE 1					✓
IR-6	CE 2					✓
IR-6	CE IR6-		✓			
IR-6	CE IR6-		✓			
IR-7	Incident Response Assistance		✓			
IR-7	CE 1					✓
IR-7	CE 2					✓
IR-8	Incident Response Plan	b. BU defined; c. BU defined frequency (at least annually]; e. BU defined		✓		
	Maintenance					
MA-1	System Maintenance Policy and Procedures	BU defined frequency based upon criticality (at least Annually)	✓			
MA-2	Controlled Maintenance		✓			
MA-2	CE 1		✓			
MA-2	CE 2					✓
MA-3	Maintenance Tools			✓		
MA-3	CE 1			✓		
MA-3	CE 2			✓		
MA-3	CE 3					✓
MA-3	CE 4					✓
MA-4	Non-Local Maintenance		✓			
MA-4	CE 1					✓
MA-4	CE 2					✓
MA-4	CE 3					✓
MA-4	CE 4					✓
MA-4	CE 5					✓
MA-4	CE 6					✓
MA-4	CE 7					✓
MA-5	Maintenance Personnel		✓			
MA-5	CE 1					✓
MA-5	CE 2					✓
MA-5	CE 3					✓
MA-5	CE 4					✓
MA-6	Timely Maintenance	BU defined as required		✓		
	Media Protection					
MP-1	Media Protection Policy and Procedures	BU defined frequency based upon criticality (at least Annually)	✓			
MP-2	Media Access	[BU Defined]	✓			
MP-2	CE 1					✓
MP-2	CE 2					✓
MP-3	Media Marking	[BU Defined]		✓		
MP-4	Media Storage					✓
MP-4	CE 1					✓
MP-5	Media Transport					✓
MP-5	CE 1					✓
MP-5	CE 2					✓
MP-5	CE 3					✓
MP-5	CE 4	GD or client sensitive information	✓			
MP-5	CE MP5-		✓			
MP-6	Media Sanitization		✓			
MP-6	CE 1					✓
MP-6	CE 2	2. BU Defined	✓			
MP-6	CE 3					✓
MP-6	CE 4					✓
MP-6	CE 5					✓
MP-6	CE 6					✓
	Physical and Environmental Protection					
PE-1	Physical and Environmental Protection Policy and Procedures	BU defined frequency based upon criticality (at least Annually)	✓			
PE-2	Physical Access Authorizations	c. Semi-annually	✓			
PE-2	CE 1					✓

	Family	Company Clarification/Defined Value	Baseline			
			Existing	All by 7/1/2012	Roadmap 7/1/2013	Not Base-lined
PE-2	CE 2					✓
PE-2	CE 3					✓
PE-3	Physical Access Control	f. BU defined; and g. BU defined based upon risk based assessment	✓			
PE-3	CE 1		✓			
PE-3	CE 2					✓
PE-3	CE 3					✓
PE-3	CE 4					✓
PE-3	CE 5					✓
PE-3	CE 6					✓
PE-4	Access Control for Transmission Medium	Not applicable to inter office CAT-5 lines				✓
PE-5	Access Control for Output Devices					✓
PE-6	Monitoring Physical Access	b. BU defined based upon risk based assessment	✓			
PE-6	CE 1					✓
PE-6	CE 2					✓
PE-7	Visitor Control		✓			
PE-7	CE 1		✓			
PE-7	CE 2					✓
PE-8	Access Records	b. BU defined based upon risk based assessment	✓			
PE-8	CE 1					✓
PE-8	CE 2					✓
PE-9	Power Equipment and Power Cabling					✓
PE-9	CE 1					✓
PE-9	CE 2					✓
PE-10	Emergency Shutoff					✓
PE-10	CE 1					✓
PE-11	Emergency Power					✓
PE-11	CE 1					✓
PE-11	CE 2					✓
PE-12	Emergency Lighting		✓			
PE-12	CE 1					✓
PE-13	Fire Protection		✓			
PE-13	CE 1					✓
PE-13	CE 2					✓
PE-13	CE 3					✓
PE-13	CE 4					✓
PE-14	Temperature and Humidity Controls	a. BU defined; and b. BU defined		✓		
PE-14	CE 1					✓
PE-14	CE 2					✓
PE-15	Water Damage Protection			✓		
PE-15	CE 1					✓
PE-16	Delivery and Removal	BU defined	✓			
PE-17	Alternate Work Site					✓
PE-18	Location of Information System					✓
PE-18	CE 1					✓
PE-19	Information Leakage					✓
PE-19	CE 1					✓
	Planning					
PL-1	Security Planning Policy and Procedures	BU defined frequency based upon criticality (at least Annually)			✓	
PL-2	System Security Plan				✓	
PL-2	CE 1					✓
PL-2	CE 2					✓
~~PL-3~~	~~System Security Plan Update~~					
PL-4	Rules of Behavior		✓			
PL-4	CE 1					✓
PL-5	Privacy Impact Assessment	OMB = CP07-105		✓		
PL-6	Security-Related Activity Planning			✓		
	Personnel Security					
PS-1	Personnel Security Policy and Procedures	BU defined frequency based upon criticality (at least Annually)	✓			
PS-2	Position Categorization					✓

	Family	Company Clarification/Defined Value	Baseline			
			Existing	All by 7/1/2012	Roadmap 7/1/2013	Not Base-lined
PS-3	Personnel Screening	b. BU defined	✓			
PS-3	CE 1					✓
PS-3	CE 2					✓
PS-4	Personnel Termination		✓			
PS-5	Personnel Transfer	BU defined	✓			
PS-6	Access Agreements	b. BU defined	✓			
PS-6	CE 1					✓
PS-6	CE 2					✓
PS-7	Third-Party Personnel Security		✓			
PS-8	Personnel Sanctions		✓			
	Risk Assessment					
RA-1	Risk Assessment Policy and Procedures	BU defined frequency based upon criticality (at least Annually)	✓			
RA-2	Security Categorization				✓	
RA-2	CE RA2-		✓			
RA-3	Risk Assessment	b. Risk Assessment Report; c. BU defined and d. Whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.		✓		
RA-3	CE RA3-GD-1		✓			
RA-3	CE RA3-GD-2		✓			
RA-3	CE RA3-GD-3		✓			
~~RA-4~~	~~Risk Assessment Update (Withdrawn)~~	Withdrawn from NIST 800-53 Rev(3)				
RA-5	Vulnerability Scanning	Credentialed Scans where appropriate. a. Refer to the Vulnerability Assessment and Patch Compliance Statistics Reporting Guidelines d. In accordance with Appendix F, Moving to Monthly Scans for internal systems by 2013		✓		✓
RA-5	CE 1		✓			
RA-5	CE 2	(2) Minimum Monthly		✓		
RA-5	CE 3					✓
RA-5	CE 4					✓
RA-5	CE 5	(5) BU defined; credentialed scans where feasible		✓		
RA-5	CE 6					✓
RA-5	CE 7					✓
RA-5	CE 8					✓
RA-5	CE 9					✓
	System and Service Acquisition					
SA-1	System and Services Acquisition Policy and Procedures	BU defined frequency based upon criticality (at least Annually)	✓			
SA-2	Allocation of Resources	a and b only		✓		
SA-3	Life Cycle Support	a only	✓			
SA-4	Acquisitions					✓
SA-4	CE 1					✓
SA-4	CE 2					✓
SA-4	CE 3					✓
SA-4	CE 4					✓
SA-4	CE 5					✓
SA-4	CE 6					✓
SA-4	CE 7					✓
SA-5	Information System Documentation		✓			
SA-5	CE 1					✓
SA-5	CE 2					✓
SA-5	CE 3					✓
SA-5	CE 4					✓
SA-5	CE 5					✓
SA-6	Software Usage Restrictions		✓			
SA-6	CE 1					✓
SA-7	User-Installed Software		✓			
SA-7	CE SA7		✓			

	Family	Company Clarification/Defined Value	Baseline			
			Existing	All by 7/1/2012	Roadmap 7/1/2013	Not Base-lined
SA-7	CE SA7		✔			
SA-8	Security Engineering Principles					✔
SA-9	External Information System Services		✔			
SA-9	CE 1					✔
SA-10	Developer Configuration Management					✔
SA-10	CE 1					✔
SA-10	CE 2					✔
SA-11	Developer Security Testing					✔
SA-11	CE 1					✔
SA-11	CE 2					✔
SA-11	CE 3					✔
SA-12	Supply Chain Protection					✔
SA-12	CE 1					✔
SA-12	CE 2					✔
SA-12	CE 3					✔
SA-12	CE 4					✔
SA-12	CE 5					✔
SA-12	CE 6					✔
SA-12	CE 7					✔
SA-13	Trustworthiness					✔
SA-14	Critical Information System Components					✔
SA-14	CE 1					✔
	System and Communication					
SC-1	System and Communications Protection Policy and Procedures	BU defined frequency based upon criticality (at least Annually)	✔			
SC-2	Application Partitioning					✔
SC-2	CE 1					✔
SC-3	Security Function Isolation					✔
SC-3	CE 1					✔
SC-3	CE 2					✔
SC-3	CE 3					✔
SC-3	CE 4					✔
SC-3	CE 5					✔
SC-4	Information in Shared Resources					✔
SC-4	CE 1					✔
SC-5	Denial of Service Protection	BU defined	✔			
SC-5	CE 1					✔
SC-5	CE 2					✔
SC-6	Resource Priority					✔
SC-7	Boundary Protection		✔			
SC-7	CE 1		✔			
SC-7	CE 2		✔			
SC-7	CE 3		✔			
SC-7	CE 4	(e) Reviews exceptions to the traffic flow policy at least annually	✔			
SC-7	CE 5		✔			
SC-7	CE 6		✔			
SC-7	CE 7			✔		
SC-7	CE 8					✔
SC-7	CE 9					✔
SC-7	CE 10					✔
SC-7	CE 11					✔
SC-7	CE 12					✔
SC-7	CE 13					✔
SC-7	CE 14					✔
SC-7	CE 15					✔
SC-7	CE 16					✔
SC-7	CE 17					✔
SC-7	CE 18					✔
SC-8	Transmission Integrity			✔		
SC-8	CE 1					✔
SC-8	CE 2					✔
SC-9	Transmission Confidentiality		✔			
SC-9	CE 1					✔

	Family	Company Clarification/Defined Value	Baseline: Existing	Baseline: All by 7/1/2012	Baseline: Roadmap 7/1/2013	Not Base-lined
SC-9	CE 2					✓
SC-10	Network Disconnect					✓
SC-11	Trusted Path					✓
SC-12	Cryptographic Key Establishment and			✓		
SC-12	CE 1					✓
SC-12	CE 2					✓
SC-12	CE 3					✓
SC-12	CE 4					✓
SC-12	CE 5					✓
SC-13	Use of Cryptography		✓			
SC-13	CE 1					✓
SC-13	CE 2					✓
SC-13	CE 3					✓
SC-13	CE 4					✓
SC-14	Public Access Protections		✓			
SC-15	Collaborative Computing Devices	BU defined		✓		
SC-15	CE 1					✓
SC-15	CE 2					✓
SC-15	CE 3					✓
SC-16	Transmission of Security Attributes					✓
SC-16	CE 1					✓
SC-17	Public Key Infrastructure Certificates			✓		
SC-18	Mobile Code					✓
SC-18	CE 1					✓
SC-18	CE 2					✓
SC-18	CE 3					✓
SC-18	CE 4					✓
SC-19	Voice Over Internet Protocol		✓			
SC-20	Secure Name /Address Resolution			✓		
SC-20	CE 1			✓		
SC-21	Secure Name /Address Resolution					✓
SC-21	CE 1					✓
SC-22	Architecture and Provisioning for		✓			
SC-23	Session Authenticity					✓
SC-23	CE 1					✓
SC-23	CE 2					✓
SC-23	CE 3					✓
SC-23	CE 4					✓
SC-24	Fail in Known State					✓
SC-25	Thin Nodes					✓
SC-26	Honeypots					✓
SC-26	CE 1					✓
SC-27	Operating System-Independent					✓
SC-28	Protection of Information at Rest					✓
SC-28	CE 1					✓
SC-29	Heterogeneity					✓
SC-30	Virtualization Techniques					✓
SC-30	CE 1					✓
SC-30	CE 2					✓
SC-31	Covert Channel Analysis					✓
SC-31	CE 1					✓
SC-32	Information System Partitioning					✓
SC-33	Transmission Preparation Integrity					✓
SC-34	Non-Modifiable Executable Programs					✓
SC-34	CE 1					✓
SC-34	CE 2					✓
	System and Information Integrity					
SI-1	System and Information Integrity Policy and Procedures	BU defined frequency based upon criticality (at least Annually)	✓			
SI-2	Flaw Remediation		✓			
SI-2	CE 1					✓
SI-2	CE 2					✓
SI-2	CE 3					✓

	Family	Company Clarification/Defined Value	Baseline			
			Existing	All by 7/1/2012	Roadmap 7/1/2013	Not Base-lined
SI-2	CE 4					✓
SI-3	Malicious Code Protection	BU defined	✓			
SI-3	CE 1		✓			
SI-3	CE 2		✓			
SI-3	CE 3			✓		
SI-3	CE 4					✓
SI-3	CE 5					✓
SI-3	CE 6					✓
SI-4	Information System Monitoring	BU defined	✓			
SI-4	CE 1		✓			
SI-4	CE 2		✓			
SI-4	CE 3					✓
SI-4	CE 4		✓			
SI-4	CE 5	BU defined		✓		
SI-4	CE 6			✓		
SI-4	CE 7					✓
SI-4	CE 8			✓		
SI-4	CE 9					✓
SI-4	CE 10					✓
SI-4	CE 11					✓
SI-4	CE 12					✓
SI-4	CE 13					✓
SI-4	CE 14					✓
SI-4	CE 15					✓
SI-4	CE 16					✓
SI-4	CE 17					✓
SI-5	Security Alerts, Advisories, and	c. BU defined	✓			
SI-5	CE 1					✓
SI-6	Security Functionality Verification					✓
SI-6	CE 1					✓
SI-6	CE 2					✓
SI-6	CE 3					✓
SI-7	Software and Information Integrity				✓	
SI-7	CE 1				✓	
SI-7	CE 2				✓	
SI-7	CE 3					✓
SI-7	CE 4					✓
SI-8	Spam Protection		✓			
SI-8	CE 1		✓			
SI-8	CE 2		✓			
SI-9	Information Input Restrictions					✓
SI-10	Information Input Validation					✓
SI-11	Error Handling					✓
SI-12	Information Output Handling and		✓			
SI-12	CE SI12		✓			
SI-13	Predictable Failure Prevention					✓
SI-13	CE 1					✓
SI-13	CE 2					✓
SI-13	CE 3					✓
SI-13	CE 4					✓
PM-1	Information Security Program Plam					✓
PM-2	Senior Information Security Officer					✓
PM-3	Information Security Resources					✓
PM-4	Plan of Action and Milestones Process					✓
PM-5	Information System Inventory					✓
PM-6	Information Security Measures of Performance					✓
PM-7	Enterprise Architecture					✓
PM-8	Critical Infrastructure Plan					✓
PM-9	Risk Management Strategy					✓
PM-10	Security Authorization Process					✓
PM-11	Mission/Business Process Definition					✓

INFORMATION SECURITY HANDBOOK	5/16/2011

INFORMATION SECURITY HANDBOOK:
APPENDIX B - SECURITY ARCHITECTURE REQUIREMENTS

1

INFORMATION SECURITY HANDBOOK	5/16/2011

Contents

2

INFORMATION SECURITY HANDBOOK	5/16/2011

3

INFORMATION SECURITY HANDBOOK	5/16/2011

1.0 Introduction

The security of a Company X's information systems is a critical component of the business process. The IT security architecture, designed to protect these information systems, must combat threats from both external and internal sources. The purpose of this appendix is to define minimum requirements to be followed by the Business Units in developing their IT security architecture.

The minimum requirements defined herein are based on a defense-in-depth approach to security. The goal is to build mutually supporting layers of defense that reduce vulnerabilities throughout the network and minimize risks - especially those resulting from single points of failure. This approach shall assist the Business Units in protecting against, detecting and reacting to the spectrum of threats facing their networks.

This appendix was developed to ensure consistent secure design, development, configuration, implementation, and operation of Company X Information Technology (IT) Infrastructures by augmenting the requirements set forth in the Information Security Handbook.

2.0 Scope

This appendix covers:

- Types of network connectivity and the guidance to define the appropriate levels of trust;
- Required elements which must be included in the security architecture;
- Hardening standards for perimeter network devices and devices in the internal network;
- Required elements which must be included in the DMZ Architecture; and
- Security requirements for data transmission, workstations, and e-mail.

Each Business Unit is required to meet the minimum standards described herein. Business Units may exceed these standards as appropriate to meet their unique business requirements.

3.0 Network Connectivity

Commercial carriers provide the majority of transmission service for Company X. The company relies on external service providers to manage these networks; however, it is ultimately the responsibility of the owner of the information, Company X, to maintain information security across these networks. As such, Business Units shall assume that third-party supplied networks are un-trusted.

3.1 Network Connectivity Requirements

3.1.1 Data Transmission

1. A BU Internal Network Segment (see Figure 1) shall utilize a switched topology (e.g.,VLANs).
2. All links that utilize un-trusted connection mediums (i.e., mediums not owned and operated by the BU) shall be encrypted.
3. The BU shall prohibit information systems from establishing simultaneous connections to multiple networks

3.1.2 Network Topology

1. Establish a physically or logically separate network for Internet only access for use by computing assets not controlled by the Business Unit.

4

2. Utilize network segmentation as required to implement secondary protection boundaries on the internal network to protect sensitive resources (e.g., Finance, Engineering, HR servers).
3. Organize the management interfaces to network devices on a separate network segment or use encryption protocols.
4. The BU shall not host any DMZ virtualized system on the same physical platform as a trusted internal network virtualized system.
5. Network System Connections. The BU CIO and Security Director shall perform a risk assessment of any new network (including significant changes) to be connected to the existing BU network, verify the connection meets the requirements in this Policy, ensure interoperability with other elements of the COMPANY X security infrastructure and architecture, and provide final approval of the connection. These steps must occur prior to connection of the new network. All trust relationships will be implemented in accordance with the appendix and terminated when networks are disconnected.
6. Connection of non-BU equipment to the BU information technology infrastructure requires the prior written authorization of the BU CIO and BU Security Director.
7. All network devices (e.g., border routers, firewalls, switches) will be company controlled devices.
8. End-of-Life Systems: The BU shall utilize only supported systems. The use of unsupported systems requires annual review and authorization by the BU CIO and Director of Security.

3.2 Network Trust Relationships

BUs must establish and document trust relationships when connecting networks.

The BU shall establish a secure boundary between the BU and each Internet point of presence and all network boundaries. Boundaries shall be established and enforced between BUs.

Trust relationships are defined as:

	Definition	Requirements
Level 1	Trusted BU internal network segment and trusted connection medium (e.g., BU on-site connections over a BU LAN)	Switched infrastructure, secure administrative protocols (e.g., Secure Shell [SSH], Kerberos)
Level 2	Un-trusted BU Networks and a trusted connection medium (e.g., on-site BU network connections to on-site research and development labs)	Firewall, Network Segmentation, switched infrastructure, secure administrative protocols (e.g., SSH, Kerberos)
Level 3	Trusted BU Internal Network segment and un-trusted connection medium (e.g., off-site collections of like organizations with central IT and IT Security control over public lines)	Encryption, secure administrative protocols (e.g., SSH, Kerberos)
Level 4	Un-trusted connecting partner and un-trusted connection medium (e.g., Company BU to Company BU, Company or Company BUs connections to partners, suppliers/vendors, and the government over public l:ines)	DMZ (program collaboration segment, if servers are shared between partners, or use of an application gateway or proxy), Firewall, Encryption, IDS, and Vulnerability Assessment
Level 5	Public facing connections (i.e., Internet) Connections to the internet are always considered un-ousted.	DMZ, Firewall, IDS (on servers in the DMZ) and Vulnerability Assessment

Note: Levels 1-3 refer to internal connections; Levels 4-5 refer to external connections. External is defined as "not controlled by the BU."

4.0 Protection of the Perimeter

This section defines the minimum requirements for the network perimeter security infrastructure.

4.1 DMZ

DMZ, or De-Militarized Zone, is a separate network segment that is established to provide additional levels of security while enabling external access by trusted or un-trusted partners to information, services, or data.

4.1.1 DMZ Reference Architecture

4.1.1 Figure 1 provides a reference architecture that provides a standardized design pattern to be used for implementing BU DMZ's and external connections. The DMZ reference architecture is segmented and consists of *access* segments, *collaboration* segments, and *service* segments. Access segments exist solely for the purpose of providing connectivity and do not contain servers. Service segments contain servers providing applications for parties permitted access to them. Program collaboration segments provide a shared resource environment for programs with external partners and customers. A DMZ implemented at a given site may contain multiple segments of various types based on the specific business requirements for that site.

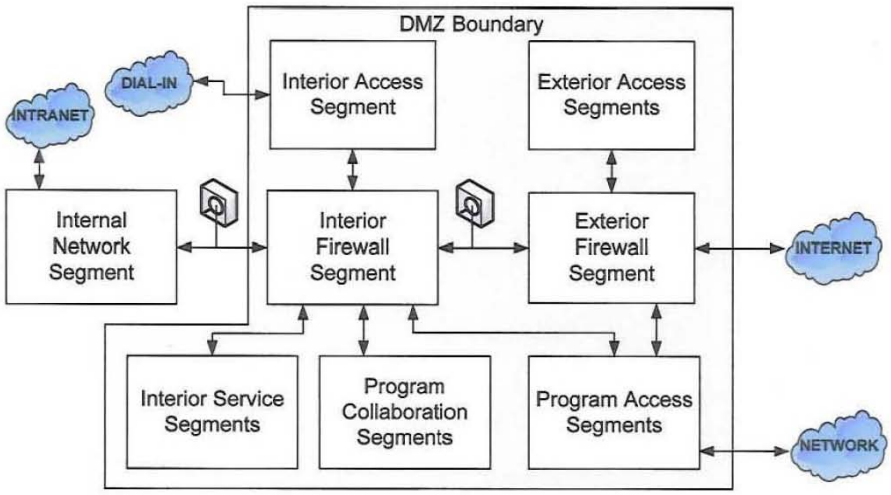

Figure 1 –DMZ Reference Architecture

DMZ segments are defined as follows:

Exterior Firewall Segment- provides the first layer of defense from hostile traffic on the Internet. Centered on the perimeter router and exterior firewall, this segment provides connection between Exterior Access Segments and the Internet and the Interior Firewall Segment and the Internet. No traffic

flow is permitted between the Exterior Access Segments and the Interior Firewall Segment. An Exterior Firewall Segment contains the following functional elements:

1. Firewall performing Layer 4 stateful filtering (Paragraph 4.2)
2. Perimeter Router performing Layer 3 IP filtering (Paragraph 4.3)
3. IDS or IDP device on the internal side of the firewall (Paragraph 4.9)
4. Optional - Traffic Shaping Device to limit traffic

These functions may be combined on common hardware given technology trends toward multifunction devices.

Exterior Access Segments - provide Internet access for program encryption equipment, foreign national visitors, and other visitors or equipment needing Internet access. Exterior Access Segments are provided access to the Internet via the Exterior Firewall Segment.

Interior Firewall Segment - controls connectivity between service and collaboration segments and internal and external networks. An Interior Firewall Segment contains the following elements:

1. Firewall performing Layer 7 protocol inspection (Paragraph 4.2)
2. Optional - Intelligent Application Gateway Appliance (Paragraph 4.5)

Interior Access Segment - provides connectivity for remote BU employees to the BUs Internal Network resources. Network access is provided via dial-up or via Internet access provided through the Exterior Firewall Segment. An Interior Access Segment may contain the following functions based on BU remote access requirements:

1. Dial-in Remote Access Servers (paragraph 4.5)
2. VPN Access Servers (Paragraph 4.5)

Interior Service Segments - provide application servers Internet access via the Exterior Firewall Segment and Interior Firewall Segment (e.g., Web, FTP, mail gateways, exterior DNS).

Program Collaboration Segments - provide application servers access by internal users located on the BU Internal Network Segment via the Interior Firewall Segment, and to external customers/partners via a Program Access Segment for program specific purposes.

Program Access Segment - provide several remote access methods of connectivity for Program Collaboration Segments. From the Interior Firewall Segment, connectivity may be permitted into a VPN concentrator device to terminate external partners and customers at the end-user level. From external sources, connectivity may be permitted from the Internet or via a partner or government owned network.

DMZs shall be configured so that a firewall shall segment them from any networks - internal and external. The routers and firewalls which segregate a DMZ from internal and external networks will restrict communications down to the specific IPs, ports, and protocols.

INFORMATION SECURITY HANDBOOK	5/16/2011

4.1.2 DMZ Requirements

1. The DMZ shall host all services required to be made accessible to the public. These services include, but are not limited to, public web sites, e-mail, external DNS, and other services required to be made accessible to the public.
2. Proxies (Proxy server or Application Layer firewall) shall be used for services which communicate between internal networks and external entities. Proxies may be bypassed when approved by the BU CIO and Director of Security. BUs shall maintain documentation of the business requirement necessitating the proxy bypass, the mitigating controls implemented to reduce the risk, and the authorization.
3. An Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS) must monitor external communications (inside and outside of the interior firewall - see Figure I) between the DMZ and internal computers.
4. Publicly accessible servers located within the DMZ must be monitored by IDS (HIDS or
5. NIDS).
6. Network taps, hubs, and switch port spans shall be utilized to feed the information to the IDS without having the IDS collecting interface addressable to the outside (refer to Paragraph 4.9).
7. Perimeter security shall restrict access to all devices based on the least access model.
8. All VPNIRAS shall be properly terminated to allow for intrusion detection monitoring of the private interface.
9. The extent of external presence, including number of DMZs and number of non-proxies addressable hosts, shall be the minimum number required to support the BU based on business requirements and IT architecture.
10. All devices must reference a single time source - utilize a Network Time Protocol (NTP) server (refer to Paragraph 4.8 for more guidance).
11. The use of end-of-life systems (non-supported) in the DMZ is prohibited. Any such operating systems or applications within the DMZ shall be replaced with a supported product prior to end-of-life.

4.2 Firewall Requirements

Firewalls are required when connections of Trust Levels 2, 4, and 5 are established (refer to Paragraph 3.2). Firewalls and other perimeter network devices which provide perimeter access control shall have rule sets that map business requirements to allowed connectivity.

1. The Perimeter Router may be used as the Exterior Firewall in addition to its routing functions if it is capable of performing Layer 4 stateful inspection.
2. A single physical firewall device may not be used to perform as both an Exterior and an Interior firewall in a DMZ.
3. Perform Stateful Layer 4 filtering.
4. Enable Layer 7 packet inspection on interior firewalls. This requirement can be performed using other network security devices (e.g., NIPS).
5. Document the business justification of all "permitted" firewall rules.
6. If SNMP is used, configure SNMP community names with read-write strings with unique names (i.e., names other than "public/private"). Disable SNMP on external interfaces.
7. Store firewall passwords in encrypted form.
8. Secure all management interfaces by prohibiting external administration from the Internet. If outside administration of the device is needed, a VPN tunnel to the internal network shall be used, and restrict management to specific IPs on the internal network.

8

9. Patch, harden, and update the operating system and firewall software in accordance with Appendix F.
10. Employ both ingress and egress firewall rules (based on least privilege access model to only allow needed services)
11. The last rule of the firewall set shall be "deny any any" (based on least privileged access model to only allow needed services).
12. Enable logging to document firewall rule violations, administrative access, configuration changes, and appropriate policy rules as defined by the BU.
13. Utilize Network Time Protocol (NTP) to synchronize all firewalls with a single time reference (refer to Paragraph 4.8).
14. Maintain and back up all updated firewall configurations and operating systems.
15. Firewalls and computing resources shall be routinely monitored to detect intrusion attempts or policy violations. This will be accomplished by use of monitoring tools and sensors as appropriate to the sensitivity of the systems.
16. Intrusion detection capability will be monitored by trained technical staff or contractor.

4.3 Perimeter Router Requirements

Perimeter routers shall meet the following security standards:

1. Perform Layer 3 filtering with minimum rules as follows:
    - External Interface Filtering Rules (Inbound)
    - DENY ANY ANY traffic with source addresses according to:
        - Internet Engineering Task Force (IETF) RFC 3330
        - IETF RFC 2267
        - IETFRFCI918
        - Additional address ranges based on current threats
    - PERMIT Destination Address Range:
        - Site Specific Addresses
    - DENY ANY shall be the last rule of the Access Control List (ACL)
    - Internal Interface Filtering Rules (Outbound)
    - PERMIT Site Specific Source Address Range
2. If the perimeter router is also being used to perform as an exterior firewall, the router must also comply with the firewall requirements in Paragraph 4.2.
3. Use Router ACLs to allow access to selected network devices based upon business requirements.
4. Document Router ACLs to identify business requirements, including duration of the rule if it is not permanently required.
5. If SNMP is used, configure SNMP community names with read-write strings with unique names (Le., names other than "public/private"). Disable SNMP on external interfaces.
6. Secure all management interfaces by prohibiting external administration from the Internet. If outside administration is required, use a VPN tunnel to the internal network if outside administration of a device is needed. Restrict management to specific IPs on the internal network. A backup interface may be used from the external interface in case the VPN tunnel is inoperative if it is restricted by IP address.
7. Store router passwords in encrypted form.
8. Patch, harden, and update operating system and device software in accordance with Appendix F.
9. Enable logging to document administrative access, configuration changes (where applicable), and appropriate policy rules as defined by the BU.

10. Utilize Network Time Protocol (NTP) to synchronize all routers with a single time reference (refer to Paragraph 4.8).
11. Maintain and back up all updated router configurations and operating systems.

4.4 Wireless Access

1. Wireless networks shall be considered a Trust Level 5 connection (refer to Paragraph 3.2). User access from the wireless network to the BU internal network segment shall be considered remote access.
2. Wireless devices connected to a BU network require the approval of the BU CIO and Security Director.
3. The BU shall configure wireless client configurations to connect only to infrastructure Access Point Networks and prohibit the use of the ad hoc mode.
4. Wireless LANs shall require network authentication in the form of a strong password (i.e. encryption key) and a network ID (SSID) to access the wireless access point. The BU shall not broadcast the SSID.
5. Wired Equivalent Privacy (WEP) is not considered adequate as the sole encryption protection for wireless networks.
6. To mitigate wireless vulnerabilities, the BU shall perform a risk assessment and security evaluation prior to implementing wireless technologies.
7. All wireless connections on a BU asset shall be automatically disabled when plugged into the BU network.

4.5 Remote Access Servers

Remote Access Servers allow authorized users to access COMPANY X information from outside the network. Requirements include:

1. Two-factor authentication as required per the Information Security Handbook,
2. NTP must be enabled per Paragraph 4.8, and
3. Logging must be enabled to document administrative and user access, configuration changes, and appropriate policy rules as defined by the BU.
4. Configure SNMP community names with read-write strings with unique names (i.e., names other than "public/private"). Disable SNMP on external interfaces.
5. Patch, update, and harden the operating system and application software in accordance with Appendix F.
6. Application level access via a "Secure Socket Layer (SSL) VPN" or "Web VPN" is authorized for users using any internet-connected computer with a web browser. SSL VPN access is restricted to specific BU designated applications.
7. Internal network level access via VPNs or dial-up will be provided only to BU furnished information assets.

Remote Access servers shall meet the following security standards:

4.5.1 Dial-in Server Requirements

1. Terminate into an Interior Access Segment and do not connect directly to an Internal Network Segment.
2. Do not permit dial-out modem connections.
3. Provide encrypted communication between the gateway and the end user.

4.5.2 VPN Concentrator Requirements

1. Terminate into an Interior Access Segment.

2. Provide encrypted runnel between the gateway and the end user.
3. Use the minimum level of encryption (See Section 6)

4.5.3 Application Gateway Requirements

1. Provide the capability to wipe a remote computer's cache of data obtained during a session.
2. Restrict user access based on least privilege model for the applications the gateway represents.
3. Patch, update, and harden the operating system and application software in accordance with Appendix F.

4.6 Service Proxies

Service proxies, whether implemented via proxy servers, appliances, or other network devices, provide internal hosts a layer of security from un-trusted external computing devices. Proxy requirements:

4.6.1 Web Proxies

All internet web traffic (i.e., http and https) shall pass through a proxy server.

4.7 Domain Name Servers (DNS)

A split DNS architecture shall be implemented when both internal (private) and external (public facing) DNS services are required so that private BU addresses are not broadcast externally. DNS Requirements:

1. DNS zone transfers shall not be permitted from an internal DNS to an external or Internet DNS server.
2. DNS enabled devices (or clients) must use Company X DNS.

4.8 Network Time Protocol (NTP)

NTP provides the IT infrastructure the ability to accurately timestamp system and device logs in the event of a security breach. NTP Requirements:

1. NTP services shall be enabled on all systems that support NTP.
2. BUs shall use a hierarchal structure to implement NTP and have at least one device that synchronizes with a minimum of a Stratum 2 time source.

4.9 Intrusion Detection

IDS monitors both authorized activity (e.g., authorized file transfers) and unauthorized activity (e.g., malicious assaults on networks or devices).

4.9.1 Host-based Intrusion Detection Requirements

1. Host-based intrusion detection is required for every internet facing server.
2. Policies shall be reviewed to ensure current and accurate reporting of events based on current infrastructure configurations.
3. The application of new intrusion detection signatures/updates shall be made within two business days after their release.

4.9.2 Network Intrusion Detection Requirements

1. Network intrusion detection sensors shall be placed as referenced in Paragraph 4.1.2.
2. Network intrusion detection is required for Trust Level 4 and Trust Level 5 network connections
3. Policies shall be reviewed to ensure current and accurate reporting of events based on current infrastructure configurations.

4. The application of new intrusion detection signatures/updates shall be made within two business days after notification.
5. All network sensors shall have their data collecting network interface set to promiscuous mode.

5.0 Servers and Workstation Requirements

This section defines the minimum requirements for servers and workstations.

1. Require a session lock after 15 minutes of inactivity (e.g., Windows password-protected screen saver)
2. The BU shall use approved tools to defend against viruses, spyware, and other malicious code on servers and end user devices when available. (Refer to Appendix E.) These tools shall be installed before collecting these systems to BU and enterprise networks
3. The BU shall implement an anti-virus program plan that, at a minimum:
   a) Has all required procedures for virus and malicious code protection
   b) Defines the process to be used when a virus infection is discovered
   c) Requires checking for updated virus signatures at least daily, preferably with an automatic push to the desktop and remote users. Push updated virus signatures within 72 hours of release.
   d) Requires scanning of removable storage media before use

5.1 Server Requirements

These guidelines provide a baseline for the BUs to follow as a minimum standard for all server installations, regardless of the platform. Configurations can be standard across a platform or unique based on a legacy or custom application. Each platform shall have a validated configuration that has been tested for both business and security functionality.

1. Harden the server per Section 7.0.
2. Enable only services (ports and protocols) that are explicitly required for applications that are installed on the server.
3. Require two-factor authentication for users accessing administrator accounts on servers, where supported by the operating system. This requirement does not apply to administrative accounts used for application-to-application transactions (e.g., service administrator accounts) or local administrative accounts via the system console.
4. Use encrypted protocols for remote administration.
5. Enable logging of failed log-on and failed access attempts.
6. Patch, update, and harden the operating system and application software in accordance with Appendix F.
7. Any configuration changes to servers, excluding patches, require the configuration to be tested and scanned for vulnerabilities. For DMZ servers, testing and scanning is required immediately after the change is implemented. For internal servers, significant changes (e.g., installing new applications) require testing and scanning within thirty days.
8. The BU shall conduct monthly vulnerability assessments of the DMZ and annual assessments of internal network and infrastructure and take prudent, cost effective actions to mitigate the identified risks to the BU. The BU shall document the remediation actions. Assessment tools are listed in Appendix E.

5.2 Workstation Requirements

Workstations including virtual desktops and thin clients (excluding smart phones, PDAs and other PEDs, reference Appendix 1) must be hardened per Section 7.0 and validated before introduction into the production environment.

INFORMATION SECURITY HANDBOOK	5/16/2011

1. Configure computers for secure remote administration and restrict users from access to local workstation administrator rights unless specifically authorized.
2. Patch, update, and harden the operating system and application software in accordance with Appendix F.
3. All workstations accessing the network remotely which are used to exchange BU or enterprise information shall use an approved personal firewall per Appendix E. The personal firewall must be operational and current at all times. The firewall product must include a central management/monitoring capability.
4. The Business Unit enforces explicit rules governing the installation of software by users.

6.0 Encryption Standard

Where required, the highest level encryption standard available should be used. At a minimum, 128-bit encryption shall be used.

7.0 Hardening Standards

Operating systems software on network devices, internal servers, and work stations/laptops shall be hardened per the CIS Level I or Legacy Standard. All application software shall be hardened to CIS application hardening standards or vendor recommendations, if provided. If the software is not covered by a CIS Standard, the BU shall select an alternative standard or develop its own hardening standard.

"Internet facing applications" are defined as all pieces of the application which face the Internet, including first, second and third tier applications that support the application environment (e.g. A backend database would be included if it supported a front-end web application). All Trust Level 4 and 5 DMZ servers shall be hardened per the CIS Enterprise or Level 2 Standard. If Enterprise or a Level 2 hardening standard is not provided by CIS, use the highest CIS Level available. If variations from the CIS Standard are required on Trust Level 4 and 5 DMZ servers for business purposes/functionality, they must be documented and approved by the BU CIO and Security Director or their designee.

It is a requirement that the Business Units:

1. Review the current CIS hardening standards, legacy standards, and vendor recommendations to determine whether the BU hardening templates should be updated on at least an annually basis.
2. Have a documented process for monitoring compliance at least quarterly to the hardening standards in place.

8.0 Communications Requirements

8.1 E-mail Requirements

8.1.1 External Mail Gateway/Relay:

1. Must be located within an Interior Service Segment (refer to Figure 1).
2. Cannot serve as the primary mail repository.
3. BUs shall utilize one or more e-mail gateways to provide external mail connectivity to internal mail servers.
4. Outgoing e-mail traffic (SMTP) shall also pass through the e-mail gateways.
5. All incoming and outgoing email attachments shall be scanned for viruses when capable.

13

INFORMATION SECURITY HANDBOOK	5/16/2011

8.1.2 Interior Mail Servers:

Must not be directly accessible via the Internet.

Must only allow the Simple Mail Transfer Protocol (SMTP) protocol when passing e-mail via the external mail gateway/relay.

8.1.3 Security of Electronic Mail (E-Mail)

The SU develops and implements procedures to address the security of e-mail communications. E-mail communications should be protected by a combination of policy, awareness, procedural and technical security controls. The BU reserves the right to monitor and to restrict e-mail activities at its sole discretion and without notice unless otherwise restricted by law.

1. BU internal e-mail shall be routed only through internal mail servers.
2. The BU shall block users from accessing external e-mail services (e.g., Hotmail, Yahoo, Google).
3. The BU shall provide users with a secure e-mail capability to transmit BU sensitive information and special category/customer designated technical data over the public Internet.
4. Email messages shall be scanned for attachments that could contain malicious code (e.g., malicious code hidden in self-extracting zip files or MPEG video clips).
5. All incoming and outgoing e-mail attachments shall be scanned for viruses
6. Users are prohibited from automatically forwarding e-mail to a non-Company account.

8.1.4 Internet E-mail Access for non-COMPANY X Assets

If a BU elects to establish and provide a network accessible e-mail service (e.g., OW A, iNotes), the BU must include appropriate security safeguards to protect all data and e-mail traffic from exposure to unauthorized persons. The security safeguards must ensure the integrity and confidentiality of the information from the mail appliance to the end-point machine and user. The minimum security safeguards must include:

1. Two factor authentication
2. Minimum encryption standards (See Section 6)
3. End-Point Security: Automatic deletion/wiping of cached files to include attachments, emails, etc., in the end-point machine (precludes exposure of COMPANY X information on public machines, kiosks, and non-COMPANY X assets)
4. Secure log-off

9.0 Telephonic Communications

The BU develops and implements procedures to address the security of telephonic communications.

1. All users conducting telephone calls to discuss BU or customer proprietary or sensitive business shall be aware of intelligence threats when using any telephone communication device.
2. When traveling, the BU shall select the appropriate telephonic methods to be used based upon the threat associated with the country in which telephonic conversations will take place. Questions regarding threat information shall be directed to the BU Director of Security.
3. The BU shall determine which programs and information are prohibited from being discussed over mobile communications. (Mobile telephone communications are insecure and easily compromised).

14

INFORMATION SECURITY HANDBOOK	5/16/2011

9.1 Digital Exchanges

The BU publishes a policy governing the management of its private or leased exchange. Digital exchanges connect both voice and data lines. This interconnection can enable a breach of voice or data to impact the other and must be protected in the same manner as data networks.

1. Perform periodic assessments of the exchange's security protection features and vulnerabilities, either by automated or manual processes.
2. Assign administrative and maintenance responsibilities to different people.
3. Restrict physical access to authorized personnel only.
4. Block remote maintenance access ports for use except by an authorized technician using policy-compliant passwords, where technically feasible. Disable the modem when not in use.
5. Use password-protected administrative console(s).
6. Use only authorized individuals for contract maintenance of BU-owned switches if company sensitive information is accessible via the switch.
7. Ensure voicemail passwords comply with the BUs password policy to the extent technically feasible. Prohibit the use of easily guessed passwords (e.g., the phone's extension or 1234).

9.2 Voice Over Internet Protocol

The BU shall conduct a risk assessment prior to the implementation of Voice over IP (VoIP).

9.3 Facsimile (FAX) Communications

The BU develops procedures to ensure both security and privacy requirements of FAX communications. The sender avoids sending sensitive, proprietary or privacy information to public FAX machines (e.g., at hotels) unless the recipient is at the machine when the FAX is sent. This is especially critical in foreign countries.

9.4 Modems

The BU shall prohibit the correction of modems to any devices in the BU without prior approval of the BU CIO and BU Security Director. BU laptops with modems do not require approval; however, laptops shall not be plugged into the BU network when connected to a phone line.

9.5 Public: Instant Messaging

The BU may authorize use of Public IM with the following requirements: Users are prohibited from downloading and executing software via IM; sending files in 1M; and transmitting proprietary, sensitive, or customer information unless the IM is end-to-end encrypted to the standard in this appendix. The BU shall implement a means of monitoring compliance with these procedures. The BU CIO and BU Security Director are the approving authorities for users to utilize Public Instant Messaging (IM) servers (e.g., AOL, Yahoo).

10.0 Personnel Requirements

The BU shall ensure that all employees or contractors who are involved with the architecture or management of the BUs information Security infrastructure receive security related training annually.

11.0 Documentation Requirements

BUs are required to maintain accurate and up-to-date documentation supporting the aspects of security architecture discussed in this appendix. Upon request from authorized personnel, the BU shall provide evidence in a timely manner that the standards in this appendix are being followed. All information related to the BU security architecture must be securely maintained.

These items include at a minimum:

11.1 Network Diagrams

At a minimum, the following items shall be depicted on the network diagram:

8. Perimeter routers, firewall s, and proxy servers;
9. Connections to public transport facilities such as: POTS, ISDN, Leased facilities such as
10. Frame Relay, ATM, ISPs, vendor supplied networks, etc.;
11. Connections to all external partner networks including other companies and how they terminate on the BU side;
12. Dial-in connections to RAS servers and their termination;
13. VPN concentrators for remote access VPN users and their termination;
14. Intrusion Detection System (IDS) and Intrusion Detection/Prevention (IOP) devices;
15. Any internet addressable servers or computers, whether they are located in the DMZ or not, and their external IP addresses;
16. All servers not on the internal network segment;
17. Authorization and access control devices (e.g., RADIUS, TACACS II, PKI);
18. All level 3 trust connections; and
19. All level 2 trust networks.

11.2 List of DMZ Servers

The list of DMZ servers shall include operating system and patch level and functions they perform.

11.3 Level 2 Trust Networks

For level 2 trust networks, document the business justification, the deviations from the information Security Handbook that exist within the level 2 trust network, and the mitigating controls that have been employed.

11.4 End-of-Life Systems

The BU shall maintain documentation of the business requirement necessitating the use of the unsupported system, the mitigating controls implemented to reduce the risk, the plan for the retirement of these systems, and the authorization.

11.5 Audit Records

The BU shall identify any additional systems, based on a business criticality and risk assessment, whose audit records will be retained as Required Information System Audit Records.

Appendix 6—Counterintelligence

For access to Appendix 6, contact the DSB office at 703-571-0081 or DSBoffice@osd.mil.